Gemeinsame Empfehlung bzgl. des Umgangs mit der EU Datenschutz-Grundverordnung (DS-GVO) im Gesundheitswesen

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.

Arbeitsgruppe Datenschutz

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Autoren

Frank DaPont	B·A·D Gesundheitsvorsorge und Sicherheitstechnik GmbH
Christoph Isele	Cerner Deutschland GmbH
Thomas Jäschke	Datatree AG
Holger Koch	Fachberater für Datenschutz und Datensicherheit
David Koeppe	Vivantes - Netzwerk für Gesundheit GmbH
Pierre Kaufmann	Agfa HealthCare GmbH
Christoph Nahrstedt	MEDNOVO Medical Software Solutions GmbH
Rainer Röhrig	Carl von Ossietzky Universität Oldenburg, Abteilungen im Department für Versorgungsforschung
Ulrich Sax	Universitätsmedizin Göttingen, Abteilung Medizinische Informatik
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Jens Schwanke	Kairos GmbH
Gerald Spyra	Kanzlei Spyra

Stand: 01.07.2016

Inhaltsverzeichnis

1. Rechtliches

1.1. Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Die Autoren sind größtenteils keine Juristen. Insofern können und dürfen sie keine rechtsverbindlichen Auskünfte geben. Daher ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen. Eine Haftung für die Angaben übernehmen die Autoren nicht. Insgesamt stellt diese Veröffentlichung keine Rechtsberatung dar und verfolgt ausschließlich den Zweck, bestimmte Aspekte anzusprechen und dafür zu sensibilisieren. Sie erhebt keinen Anspruch auf Vollständigkeit. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen für die jeweilige Situation anhand der geltenden rechtlichen Vorschriften geprüft und angepasst werden.

1.2. Urheber- und Kennzeichenrecht

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen. Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer.

Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind.

1.3. Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

Dieses Werk ist unter einer Creative Commons-Lizenz (4.0 Deutschland Lizenzvertrag) lizenziert.

D. h. Sie dürfen:

- Teilen: das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen, solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.

Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

http://creativecommons.org/licenses/by/4.0/deed.de

2. Vorwort

Der von der Kommission erarbeitete Vorschlag zu einer europäischen Datenschutz-Grundverordnung (DS-GVO) stammt aus dem Januar 2012, Vorarbeiten dazu gehen noch einige Jahre weiter zurück. Die Zeit zwischen Januar 2012 und Dezember 2015 wurde für das Suchen nach Kompromissen zwischen den verschiedenen Meinungen von EU-Kommission, EU-Parlament und EU-Ministerrat verwendet. Die Verordnung wird zwei Jahre nach ihrem In-Kraft-Treten gelten, also am 25. Mai 2018. D. h. die DS-GVO erforderte eine „Geburtszeit" von knapp 10 Jahren. In diesen 10 Jahren ist die Entwicklung in der Welt nicht stehen geblieben, sodass die Verordnung in einigen Punkten schon zum Zeitpunkt ihrer Verabschiedung veraltet wirkt.

Die DS-GVO übernimmt im Kern die aus der Richtlinie 95/46/EG („Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr") bekannten datenschutzrechtlichen Grundprinzipien: Die Grundsätze der „Datenvermeidung und Datensparsamkeit", der „Zweckbindung", des „Verbots mit Erlaubnisvorbehalts" und der „Transparenz" finden sich auch im neuen Regelungskonzept wieder.

Eine Einschätzung der Auswirkungen der DS-GVO ist schwierig: es existieren derart viele Öffnungsklauseln, dass eine Darstellung der Anforderungen der Verordnung nur in Abhängigkeit zu der jeweiligen nationalen Umsetzung möglich ist. Hieraus folgt unmittelbar, dass die Zielsetzung einer europaweit geltenden Datenschutzgesetzgebung verfehlt wurde.

Bei der Interpretation der DS-GVO muss man dem üblichen juristischen Vorgehen bei der Interpretation von Gesetzestexten folgen:

1) Grammatische Auslegung - „Der Wortlaut"
2) Historische Auslegung - „Die Gesetzgebungsgeschichte"
   - Die Anforderungen der Datenschutzrichtlinie dürfen nicht unterschritten werden
3) Systematische Auslegung - „Die Systematik des Gesetzes"
4) Teleologische Auslegung - „Der Sinn und Zweck"
   - Begründung durch den Gesetzgeber, insbesondere
     - Förderung der Binnenmarktdimension des Datenschutzes;
     - Verringerung des Verwaltungsaufwandes für Unternehmen
     - Harmonisierung Datenschutzrecht in der EU

Dabei steht die Interpretation des Wortlautes grundsätzlich an erster Stelle, d. h. wenn der Gesetzestext eindeutig ist oder etwas anderes als die Begründung des Gesetzgebers aussagt, so gilt der Gesetzestext. In der DS-GVO wird zudem des Öfteren auf „öffentliches Interesse" und „Verhältnismäßigkeit" verwiesen, daher wird auf diese Begrifflichkeiten ebenfalls näher eingegangen.

Die vorliegende Ausarbeitung beruht auf der offiziellen Übersetzung[1].

[1] EUR-LEX: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Online, zitiert am 2016-05-13; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.DEU&toc=OJ:L:2016:119:TOC

3. Management Summary

1) Zielsetzung der DS-GVO ist ein wirksamer Schutz personenbezogener Daten vor unbefugtem Zugriff, wobei „der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden“ darf (Art. 1 Abs. 3 DS-GVO). Dies erfordert
    a. eine Stärkung und Präzisierung der Rechte der betroffenen Personen (ErwGr. 11)
    b. eine Verschärfung der Auflagen für Verantwortliche bzgl. der Datenverarbeitung (ErwGr. 11)
    c. europaweit gleiche Befugnisse bei der Überwachung und Gewährleistung der Einhaltung der Vorschriften zum Schutz personenbezogener Daten (ErwGr. 11)
    d. europaweit gleiche Sanktionen im Falle einer Verletzung des Schutzes personenbezogener Daten (ErwGr. 11)
2) Die Verordnung ist ab dem 25. Mai 2018 unmittelbar geltendes Recht in ganz Europa und genießt grundsätzlich Anwendungsvorrang vor jedem nationalen Gesetz. Aber die DS-GVO weist nationale Öffnungsklauseln auf, sodass in diesen speziellen Bereichen nationale Anpassungen ermöglicht werden.
3) Grundsätze in Bezug auf Verarbeitung personenbezogener Daten bleiben erhalten, insbesondere gilt:
    a. Weiterhin Verbot mit Erlaubnisvorbehalt, d. h. Rechtmäßigkeit einer Verarbeitung muss geprüft werden
    b. Voraussetzung Rechtmäßigkeit: Zweckbindung bei Datenminimierung bei gleichzeitiger Begrenzung der Speicherdauer
    c. Verarbeitung nur entsprechend Treu und Glauben
4) Die Verordnung verursacht Anpassungsbedarf
    a. Verordnung führt z.T. neue Begriffe / Definitionen ein, bereits bekannte Begrifflichkeiten werden z.T. abweichend vom bisherigen deutschen Recht definiert und erfordern daher eine neue Auslegung
    b. Auftragsdatenverarbeitung (Vertragsgestaltung, Änderungen bei Rechten und Pflichten, ggfs. gemeinsame Haftung von Auftraggeber und Auftragnehmer, hohes Bußgeld bei fehlerhafter Auftragsverarbeitung sowohl für Auftraggeber wie Auftragnehmer möglich)
    c. Neue Pflichten bzgl. Verarbeitung personenbezogener Daten (z. B. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)
    d. Ggfs. zwingende Einbeziehung der Datenschutzaufsichtsbehörde, falls Datenschutz-Folgenabschätzung ein hohes Risiko aufzeigt (Verstoß kann hohes Bußgeld verursachen)
    e. Einwilligungen (Anpassung Informationspflichten, hohes Bußgeld bei Verarbeitung mit fehlender oder fehlerhafter Einwilligung)
    f. Neue Betroffenenrechte (z. B. Datenübertragbarkeit) sowie Erweiterung bestehender Rechte (überwiegend Informationspflichten), Fehler bei der Wahrung von Betroffenenrechten sind bußgeldbewehrt
    g. Anpassung der internen Dokumentation entsprechend Vorgaben der DS-GVO (fehlende / fehlerhafte Dokumentation bußgeldbewehrt)
5) Sanktionen durch Bußgelder wurden massiv verschärft
    a. einerseits Bußgelder deutlich erhöht (bis zu 10 bzw. 20 Mio. Euro bzw. 2%/4% des weltweiten Vorjahresumsatzes, je nachdem, was höher ist)
    b. Bußgeldtatbestände deutlich erweitert
    c. Pflicht zum Bußgeld verankert, d. h. bei Verstoß muss ein Bußgeld angeordnet werden (bisher in Deutschland „Kann-Regelung“)

4. Allgemeines zur DS-GVO

4.1. Entwicklung der DS-GVO: die Historie

- 23.11.1995: Veröffentlichung Richtlinie 95/46/EG (Datenschutzrichtlinie)
- 25.01.2012: Europäische Kommission stellt EU-Datenschutzreform vor, Zielsetzung
  - Stärkung des Datenschutzes innerhalb der EU bei gleichzeitiger
  - Vereinheitlichung der europäischen und nationalen Datenschutzvorschriften;
  - Förderung der Binnenmarktdimension des Datenschutzes;
  - Verringerung des Verwaltungsaufwandes für Unternehmen.

  Umsetzung durch zwei Rechtsakte:
  - EU-Richtlinie für polizeiliche und justizielle Zusammenarbeit in Strafsachen
  - Datenschutz-Grundverordnung regelt alles andere
- 30.03.2012: Subsidiaritätsrüge deutscher Bundesrat: Vorschlag verstoße gegen Art. 5 Abs. 3 des Vertrags über die Europäische Union (EUV)
- 21.10.2013: Europäische Parlament veröffentlicht seine Position bzgl. Verordnung
- 12.03.2014: EU-Parlament nimmt Reform in erster Lesung an
  Mitgliedsstaaten lehnen den Vorschlag des EU-Parlaments ab
- 15.06.2015: EU-Ministerrat einigt sich auf Position bzgl. Verordnung
- 09.10.2015: Justizminister der EU-Mitgliedsstaaten einigen sich bzgl. Datenschutzrichtlinie
- 15.12.2015: : Abstimmung bzgl. Verordnung zwischen Rat, Europäischem Parlament und Europäischer Kommission (sogenannter Trilog) erfolgreich: Einigung von Kommission, Ministerrat und Parlament auf eine gemeinsame Fassung
- 17.12.2015: Ausschuss LIBE stimmte der Trilog-Fassung zu
- 21.12.2015: Ausschuss des EU-Ministerrats stimmte der Trilog-Fassung zu
- 28.01.2016: Übersetzungen des Trilog-Ergebnisses in die EU-Sprachen steht auf dem Server von EUR-Lex zur Verfügung
- 21.04.2016: Formeller Abschluss der ersten Lesung
- 06.04.2016: Offizielle Übersetzung in Sprachen der EU für Abstimmung Rat/Parlament
- 08.04.2016: Erste Lesung im Rat, Standpunkt Rat fixiert
- 12.04:2016: Finale Abstimmung im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE)
- 14.04.2016: Abstimmung bzgl. Annahme im Plenum des Parlaments
- 04.05.2016: Veröffentlichung im europäischen Amtsblatt
- 25.05.2016: Inkrafttreten der Verordnung
- 25.05.2018: Ende der Übergangsfrist und unmittelbare Geltung der DS-GVO in Europa

4.2. Struktur der EU Datenschutz-Grundverordnung

Kapitel 1: Allgemeine Bestimmungen
Artikel 1 bis 4

Kapitel 2: Grundsätze
Artikel 5 bis 11

Kapitel 3: Rechte der betroffenen Person
Artikel 12 bis 23

Abschnitt 1: Transparenz und Modalitäten
Artikel 12

Abschnitt 2: Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten
Artikel 13 bis 15

Abschnitt 3: Berichtigung und Löschung
Artikel 16 bis 20

Abschnitt 4: Widerspruchsrecht und automatisierte Entscheidung im Einzelfall
Artikel 21 bis 22

Abschnitt 5: Beschränkungen
Artikel 23

Kapitel 4: Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter
Artikel 24 bis 43

Abschnitt 1: Allgemeine Pflichten
Artikel 24 bis 31

Abschnitt 2: Sicherheit personenbezogener Daten
Artikel 32 bis 34

Abschnitt 3: Datenschutz-Folgenabschätzung und vorherige Konsultation
Artikel 35 bis 36

Abschnitt 4: Datenschutzbeauftragter
Artikel 37 bis 39

Abschnitt 5: Verhaltensregeln und Zertifizierung
Artikel 40 bis 43

Kapitel 5: Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen
Artikel 44 bis 50

Kapitel 6: Unabhängige Aufsichtsbehörden
Artikel 51 bis 59

Abschnitt 1: Unabhängigkeit
Artikel 51 bis 54

Abschnitt 2: Zuständigkeiten, Aufgaben und Befugnisse
Artikel 55 bis 59

4.3. EU-Verordnung vs. deutsches Recht

Es wird in Deutschland die Frage gestellt , in welchem Verhältnis die DS-GVO zu den vom Bundesverfassungsgericht im Recht auf informationelle Selbstbestimmung festgehaltenen Grundrecht steht und ob die verfassungsrechtlichen Vorgaben innerhalb der DS-GVO beachtet werden, d. h. ob die DS-GVO mit dem deutschen Grundgesetz vereinbar ist.

Das ursprüngliche Urteil zur informationellen Selbstbestimmung war im Kern als Abwehrrecht des Einzelnen gegen staatliche Datensammlung gedacht, d. h. ein Verfassungsrecht, um den Bürger gegen Übergriffe des Staates zu schützen. Die DS-GVO hingegen ist eine Regulierung hinsichtlich der privatwirtschaftlichen Datenverarbeitung. Somit ist die Frage, ob diese Regelung dem Anspruch des Verfassungsrechts der informationellen Selbstbestimmung überhaupt genügen kann.

Weiterhin bietet die DS-GVO bedingt durch die vielen Öffnungsklauseln ein breites Spektrum an Ausgestaltungsmöglichkeiten, sodass auch infrage gestellt ist, ob das verfassungsrechtlich geforderte Mindestmaß an Rechtssicherheit und insbesondere auch Rechtsklarheit durch die DS-GVO gegebenen ist.

4.3.1. (Nationale) Öffnungsklauseln in der DS-GVO

Die Berücksichtigung gewisser nationaler aber auch wirtschaftlicher Interessen spielte bei den Verhandlungen rund um die Regelungen der DS-GVO eine große Rolle[2]. .

Um den „nationalen“ Interessen der Mitgliedsstaaten ausreichend Rechnung zu tragen, wurde deshalb in den entsprechenden Regelungen der DS-GVO vielfach der Ansatz „Verlagerung der Gesetzgebung auf den nationalen Gesetzgeber“ gewählt. Für gewisse, oftmals sehr komplexe und „brisante“ Datenschutzsachverhalte wurde deshalb die Gesetzgebungskompetenz mittels der „nationalen Öffnungsklauseln“ auf den nationalen Gesetzgeber übertragen.

Vereinfacht gesagt geben „nationale Öffnungsklauseln“ den nationalen Gesetzgebern die Möglichkeit bzw. verpflichten sie, für bestimmte Sachverhalte / Bereiche, eigene nationale Regelungen zu schaffen, die dann die Regelungen der DS-GVO ausfüllen bzw. sie ergänzen. Diese nationalen (neuen oder aus dem bisherigen Recht übernommenen bzw. modifizierten) Regelungen gehen den allgemeineren Regelungen der DS-GVO vor.

Der Vorrang dieser nationalen Regelungen geht jedoch wiederum immer nur soweit, wie der „Öffnungsbereich“ der Klauseln in der DS-GVO dies zulässt. So ist es bspw. wiederum nicht möglich, dass eine nationale Regelung gewisse Sachverhalte (abweichend) regelt, die schon durch die DS-GVO abschließend geregelt wurden.

Wie die DS-GVO an vielen Stellen betont, muss stets auch gewährleistet sein, dass die nationalen Regelungen mit den Regelungen der DS-GVO harmonieren, d. h. als „verhältnismäßig“ anzusehen sind. Weiterhin müssen sie einem „legitimen“ nationalen Interesse dienen und die neuen (nationalen) Regelungen dürfen dem Verordnungstext nicht widersprechen.

„Nationale Öffnungsklauseln“ lassen sich relativ „einfach“ am Wortlaut erkennen. Formulierungen wie: „*nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen*“ stellen nationale Öffnungsklauseln dar.

[2] Mag. Maximilian Schrems (2013) „Forum Shopping” für die IT-Industrie? Online, zitiert am 2016-05-13; Verfügbar unter http://www.europe-v-facebook.org/IMCO_pub_de_ON.pdf

Der Effekt, den nationale Öffnungsklauseln haben können, lässt sich schnell an „aktuellen Anwendungsfällen“ verdeutlichen. So können etwa durch nationale Öffnungsklauseln theoretisch „Big Data-Analysen“ oder Anwendungen im „Internet der Dinge“, die einen großen gesellschaftlichen Mehrwert versprechen (und daher durchaus im öffentlichen Interesse liegen könnten) durch entsprechende nationale Gesetze legitimiert werden, auch wenn sie eigentlich bei eng ausgelegtem Zweckbindungsgrundsatz entsprechend den Vorgaben der DS-GVO eigentlich unzulässig wären. Da die von den nationalen Öffnungsklauseln erfassten Regelungen nationales, mit der DS-GVO in Einklang stehendes Recht sind, sind die entsprechenden Regelungen bindend für alle Beteiligten wie „Verantwortliche“, Auftragsverarbeiter Aufsichtsbehörden (auch anderer Staaten) usw.. Dies gilt solange, wie diese nationale Gesetzgebung nicht außer Kraft gesetzt wurde, bspw. durch das BVerfG oder den EUGH.

Ob und wie ein Gesetzgeber durch die von den „nationalen Öffnungsklauseln“ eröffneten Möglichkeiten Gebrauch macht, bleibt abzuwarten. Nach ersten Einschätzungen müssen jedenfalls alleine in Deutschland ca. 300 Gesetze / Verordnungen / Richtlinien mehr oder weniger intensiv an die DS-GVO angepasst werden[3].

Wenn jedoch einige oder alle Mitgliedstaaten von der Möglichkeit, eigene Regelungen zu treffen Gebrauch machen, würde die Frage der Zulässigkeit der hiervon erfassten Datenverarbeitung innerhalb der EU höchstwahrscheinlich unterschiedlich beantwortet werden müssen. Die DS-GVO ist durch ihre vielen Öffnungsklauseln eher als ein „Mischung“ zwischen EU-Verordnung und Richtlinie oder als eine „Richtlinie im Gewand einer Verordnung“ anzusehen.

Verantwortliche tun deshalb gut daran, auch nach Geltung der DS-GVO-Regelungen (wie bisher) bei Übermittlungen von Daten zu Zwecken, die von nationalen Öffnungsklauseln erfasst werden, besonders kritisch zu überprüfen, ob und wie dieses und die weitere Verarbeitung nach dem jeweils geltenden nationalen Recht zulässig ist.

Die DS-GVO sieht an einer ganzen Reihe zentraler Regelungspunkte die Möglichkeit vor, durch nationales Recht Sonderregelungen zu schaffen. Nationale Anpassungen sind z. B. bei folgenden Punkten möglich:

1) Details zur Definition der „verantwortlichen Stelle“
   (Artikel 4 Abs. 7 „Begriffsbestimmungen“)
2) Details zur Definition des „Empfängers“
   (Artikel 4 Abs.9 „Begriffsbestimmungen“)
3) Erlaubnistatbestände zur Verarbeitung personenbezogener Daten
   (Artikel 6 „Rechtmäßigkeit der Verarbeitung“, Abs. 2, 3, 4)
4) Absenkung der Altersgrenze zur Einwilligung durch Kinder auf bis zu 13 Jahre
   (Artikel 8 „Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft“, Abs. 1)
5) Ausgestaltung gesonderter nationaler Erlaubnistatbestände zur Verarbeitung besonderer Arten personenbezogener Daten
   (Artikel 9 „Verarbeitung besonderer Kategorien personenbezogener Daten“, Abs. 2 Lit. a, b, g, h, i und j sowie Abs. 3 und 4)

[3] Handelsblatt. (2015) Europa treibt den Datenschutz voran. Online, zitiert am 2016-05-13; Verfügbar unter http://www.handelsblatt.com/politik/international/facebook-google-und-die-eu-europa-treibt-den-datenschutz-voran/11919262.html

6) Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln
   (Artikel 10 „Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten“)
7) Nationale Spezialregelung (inkl. der Möglichkeit zur Einschränkung) der Informationsansprüche des Betroffenen
   (Artikel 14 „Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden“, Abs. 5 Lit. c und d)
8) Einschränkung des Rechts auf Datenlöschung des Betroffenen
   (Artikel 17 „Recht auf Löschung ("Recht auf "Vergessenwerden")“, Abs. 1 Lit. e und Abs. 3 Lit. b)
9) Beschränkung des Rechts auf Einschränkung der Verarbeitung
   (Artikel 18 „Recht auf Einschränkung der Verarbeitung“, Abs. 2)
10) Einschränkung des Verbots der automatisierten Einzelentscheidungen bzw. Zulässigkeit des Profilings durch nationales Recht
    (Artikel 22 „Automatisierte Entscheidungen im Einzelfall einschließlich Profiling“, Abs. 2 Lit. b)
11) Einschränkung aller Betroffenenrechte
    (Artikel 23 „Beschränkungen“, Abs. 1)
12) Aufgaben der Verantwortlichen
    (Artikel 26 „Gemeinsam für die Verarbeitung Verantwortliche“, Abs. 1)
13) Rechtsgrundlage der Auftragsverarbeitung
    (Artikel 28 „Auftragsverarbeiter“, Abs. 3)
14) Rückgabe der Daten an den Auftraggeber
    (Artikel 28 „Auftragsverarbeiter“, Abs. 3 Lit. g)
15) Einbindung von Unterauftragnehmern
    (Artikel 28 „Auftragsverarbeiter“, Abs. 4)
16) Schaffung nationaler Datenverarbeitungsvorgaben für Auftragsverarbeiter
    (Artikel 29 „Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters“)
17) Möglichkeit zur Verschärfung der Regeln hinsichtlich der Durchführung von Vorabkontrollverfahren für neue datenverarbeitende Systeme
    (Artikel 35 „Datenschutz-Folgenabschätzung“, Abs. 10)
18) Konsultation der Aufsichtsbehörden je nach Ergebnis der Datenschutz-Folgenabschätzung
    (Artikel 36 „Vorherige Konsultation“, Abs. 5)
19) Erweiterung der Bestell-Voraussetzungen eines Datenschutzbeauftragten
    (Artikel 37 „Benennung eines Datenschutzbeauftragten“, Abs. 4)
20) Verpflichtung des Datenschutzbeauftragten zur Geheimhaltung bzw. Vertraulichkeit
    (Artikel 38 „Stellung des Datenschutzbeauftragten“, Abs. 5)
21) Internationale Übereinkunft zur Datenübermittlung in ein Drittland
    (Artikel 48 „Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung“)
22) Erleichterung von Datentransfers an Stellen außerhalb der Europäischen Union
    (Artikel 49 „Ausnahmen für bestimmte Fälle“, Abs. 1 Lit. g sowie Abs. 4 und 5)
23) Einrichtung einer Datenschutz-Aufsichtsbehörde
    (Artikel 54 „Errichtung der Aufsichtsbehörde“ Abs. 1)
24) Bestimmung der Verschwiegenheitspflicht der Datenschutz-Aufsichtsbehörde
    (Artikel 54 „Errichtung der Aufsichtsbehörde“ Abs. 2)

25) Zutrittsrecht zu Geschäftsräumen der Datenschutz-Aufsichtsbehörden
(Artikel 58 „Befugnisse“, Abs. 1 Lit. f)
26) Zusätzliche Befugnisse von Datenschutz-Aufsichtsbehörden
(Artikel 58 „Befugnisse“, Abs. 6)
27) Bekanntgabe der Tätigkeitsberichte der Datenschutz-Aufsichtsbehörde
(Artikel 59 „Tätigkeitsberichte“)
28) Regelungen bzgl. Ablehnung der Ersuchung um Amtshilfe anderer Aufsichtsbehörden
(Artikel 61 „Gegenseitige Amtshilfe“, Abs. 4 Lit. b)
29) Tätigkeit einer Aufsichtsbehörde in einem anderen Mitgliedsland
(Artikel 62 „Gemeinsame Maßnahmen der Aufsichtsbehörden“ Abs. 3 und 4)
30) Vertretung von betroffenen Personen bei Wahrnehmung dessen Rechte
(Artikel 80 „Vertretung von betroffenen Personen“, Abs. 1 und 2)
31) Die Entscheidung, ob Bußgelder nicht nur für Privatunternehmen, sondern auch für Behörden oder öffentliche Einrichtungen verhängt werden können, wird vollständig in die Verantwortung der Mitgliedstaaten gelegt
(Artikel 83 „Allgemeine Bedingungen für die Verhängung von Geldbußen“, Abs. 7)
32) Festlegung von Sanktionen bei Verstößen gegen Datenschutzrecht
(Artikel 84 „Sanktionen“, Abs. 1)
33) Schaffung nationaler Ausnahmen von Regelungsgrundsätzen bei Datenverarbeitungsvorgängen für journalistische Zwecke
(Artikel 85 „Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit“)
34) Einsichtnahme in öffentliche Dokumente, die personenbezogene Daten enthalten
(Artikel 86 „Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten“)
35) Spezifische Ausgestaltung bei Verwendung einer nationalen Identifizierungsnummer
(Artikel 87 „Verarbeitung der nationalen Kennziffer“)
36) Schaffung nationaler Spezialregelungen bei der Verarbeitung von Beschäftigtendaten
(Artikel 88 „Datenverarbeitung im Beschäftigungskontext“)
37) Beschränkung der Betroffenenrechte bzgl. Datennutzung zu Archivzwecken, Forschung und statistischen Zwecken
(Artikel 89 „Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken“, Abs. 2)
38) Schaffung nationaler Ausnahmen von Regelungsgrundsätzen bei Datenverarbeitungsvorgängen für Archivzwecken, Forschung und statistischen Zwecken
(Artikel 89 „Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken“, Abs. 3)
39) Schaffung besonderer nationaler Geheimhaltungsverpflichtungen
(Artikel 90 „Geheimhaltungspflichten“, Abs. 1)

4.4. Interpretation der DS-GVO

Klassisch existieren vier Methoden zur Auslegung von rechtlichen Bestimmungen:

- Grammatische Auslegung:
  Was sagt der Wortlaut der Gesetzesbestimmung aus?
- Historische Auslegung:
  Wie entwickelten sich die Inhalte der Gesetzesbestimmung? Wie ist die Gesetzgebungsgeschichte?
- Systematische Auslegung:
  Wie ist die Systematik der Gesetzesbestimmung? In welchem Zusammenhang steht die Gesetzesbestimmung? Was führte zu der Gesetzesbestimmung?
- Teleologische Auslegung:
  Was ist der Sinn der Gesetzesbestimmung? Was der Zweck? Was wollte der Gesetzgeber erreichen?

Unabhängig davon bildet das Grundgesetz die höchste Rechtsnorm innerhalb Deutschlands. Die Auslegung eines Gesetzestextes muss daher immer verfassungskonform erfolgen und darf nicht gegen Bestimmungen des Grundgesetzes verstoßen. Allerdings endet die Möglichkeit, eine Gesetzesbestimmung verfassungskonform auszulegen dort, wo die Auslegung dem Wortlaut und dem klar erkennbaren Willen des Gesetzgebers widerspricht. Somit ist die erste Stufe der Interpretation einer Gesetzesbestimmung immer der Wortlaut.

4.4.1. Grammatische Auslegung: Wortlaut und Übersetzung

Die gesamte Verhandlung der DS-GVO erfolgte in englischer Sprache, auch der abschließende Trilog sowie die Einigung wurde in englischer Sprache geführt. Wenn in die EU-Landessprache übersetzte Textstellen daher europaweit nicht eindeutig sind (z. B. Abweichung französische und spanische Übersetzung), dann wird entscheidend sein, was im englischen „Originaltext“ steht, also was das Trilog-Verhandlungsergebnis war. Daher muss ggfs. bei der Interpretation neben dem offiziellen deutschen Text auch der englische Text Beachtung finden.

4.4.2. Teleologische Auslegung

Hinsichtlich der Interpretation der Datenschutz-Grundverordnung müssen bei der Auslegung insbesondere die Erwägungsgründe herangezogen werden, denn hier sind die Gründe bzgl. einer teleologischen Auslegung zu erfahren: in den Erwägungsgründen beschreibt der europäische Gesetzgeber, was er mit der Verordnung erreichen wollte.

4.4.3. Europäisches Recht = europäische Auslegung

Die DS-GVO ist kein deutsches, sondern europäisches Recht. D. h. das Recht muss in allen zur EU gehörenden Ländern gleich ausgelegt werden. Daher ist stets zu prüfen: wie wird der Verordnungstext in anderen Ländern interpretiert? Was sagt die Mehrheit?

Insbesondere unter Berücksichtigung der Tatsache, dass der künftige Datenschutzausschuss im Prinzip wie die Artikel-29-Datenschutzgruppe von Vertretern der nationalen Aufsichtsbehörden besetzt wird, muss den Auslegungen der Artikel-29-Datenschutzgruppe bzgl. den Bestimmungen der RL 95/46/EG, die sich im Vergleich zur DS-GVO nicht oder nur minimal änderten, eine besondere Beachtung geschenkt werden.

5. Geltungsbereich der DS-GVO

Der sachliche und räumliche Anwendungsbereich der europäischen Datenschutz-Grundverordnung ist im Wesentlichen in Art. 2 und 3 DS-GVO geregelt.

5.1. Sachlicher Anwendungsbereich

Fundstelle in der DS-GVO:

- Art. 2 „Sachlicher Anwendungsbereich“

Kommentar:

Der sachliche Anwendungsbereich umfasst die vollständige oder teilweise automatische Verarbeitung personenbezogener Daten. Nicht-automatisierte Verarbeitung von Daten wird ebenfalls von der Verordnung erfasst, wenn diese Daten in einer Datei gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DS-GVO). Ausnahmen gelten insbesondere für die Bereiche der nationalen Sicherheit, der Verfolgung von Straftaten und der Datenverarbeitung durch natürliche Personen zu ausschließlich persönlichen oder familiären Zwecken.

Eine dem § 1 Abs. 3 BDSG vergleichbare Abgrenzungsnorm zu vorrangigen spezialdatenschutzrechtlichen Normen ist in der DS-GVO nicht vorgesehen. Die uns vom BDSG her bekannte Rolle des subsidiären „Auffangnetzes” ist somit zukünftig nicht mehr gegeben.

Der einzige Artikel der DS-GVO, welcher eine sachliche Abgrenzung des Datenschutzes zum Berufsrecht vorsieht, ist Art. 84 Abs. 1 DS-GVO. Hiernach wird den Mitgliedstaaten das Recht eingeräumt, die Befugnisse der Aufsichtsbehörde dahingehend zu regeln, dass dem Schutz von Berufsgeheimnissen oder anderen gleichwertigen Geheimhaltungspflichten Rechnung getragen wird.

5.2. Räumlicher Anwendungsbereich

Fundstelle in der DS-GVO:

- Art. 3 „Räumlicher Anwendungsbereich“

Kommentar:

Im Vergleich zum bisherigen deutschen Recht erfolgt eine Erweiterung des räumlichen Anwendungsbereichs. Art. 3 Abs. 1 DS-GVO: „Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines für die Verarbeitung Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet“ (Niederlassungsprinzip).

Die DS-GVO findet damit auch dann Anwendung, wenn ein Anbieter in einem nicht europäischen Drittstaat (z. B. die USA) Daten verarbeitet, um Dienste oder Waren Personen anzubieten, die innerhalb der EU ansässig sind („Marktortsprinzip“). Zum einen genügt somit ein Angebot von Waren oder Dienstleistungen (Art. 3 Abs. 2 Lit. a DS-GVO), auch wenn von der betroffenen Person keine Zahlung zu leisten ist. Damit werden die meisten geldfreien Internet-Dienstleistungen wie Suchdienste und soziale Netzwerke von den Vorschriften der DS-GVO erfasst. Zum anderen wird eine Verhaltensbeobachtung nur erfasst, „soweit das Verhalten in der Europäischen Union erfolgt” (Art. 3 Abs. 2 Lit. b DS-GVO). Dabei findet das Verhalten immer in der Union statt, wenn sich die betroffene Person in der Union physisch aufhält. Somit fallen auch Handlungen in der virtuellen Welt des Internets unter die Regelungen der DS-GVO, unabhängig von den Serverstandorten.

6. Erläuterungen zu Begrifflichkeiten der DS-GVO

6.1. Personenbezug: Änderung bei Begriff der Anonymität

Kommentar:

Nach der noch geltenden Definition des BDSG und einigen anderen Datenschutzregelungen sind personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.

Die DS-GVO hingegen hat einen anderen Weg / Ansatz gewählt. Sie zollt der Tatsache Tribut, dass Daten Träger unterschiedlichster Informationen sind und hat sich deshalb vom reinen „Einzelangaben“-Ansatz weitgehend verabschiedet. Nach der DS-GVO sind personenbezogene Daten deshalb „alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person ("betroffene Person") beziehen“. Da „Informationen“ natürlich auch „Einzelangaben“ sein können, ist die Definition des BDSG in dieser Begriffsbestimmung auch enthalten.

Wie bei den derzeit geltenden Datenschutzregelungen ist beim Personenbezug weiterhin „Dreh und Angelpunkt“ die „Bestimm-“ bzw. „Identifizierbarkeit“ der Person mittels der aus den Daten gewonnenen Informationen.

So ist eine Person nach der DS-GVO identifizierbar, *„die direkt oder indirekt, insbesondere mittels Zuordnung wie Namen, Kennnummer, Standortdaten, Online-Kennung (IP-Adresse) oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität ist.*“

Ob eine Person somit als identifizierbar anzusehen ist oder nicht, kann jeweils nur im Einzelfall bestimmt werden. Letztlich gilt entsprechend des Textes der DS-GVO: existiert eine Möglichkeit zur Identifizierung, so gilt eine Identifizierung als möglich und es handelt sich im Sinne der DS-GVO um einen Personenbezug.

Zur Auslegung der DS-GVO sind die Erwägungsgründe heranzuziehen. D. h., wenn man nicht sicher beurteilen kann, ob eine Identifikation möglich ist oder nicht, so ist die Möglichkeit anhand der in den Erwägungsgründen genannten Kriterien zu beurteilen. Nach Erwägungsgrund 26 sind bei der Frage der Identifizierbarkeit *„alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die Person direkt oder indirekt zu identifizieren, …*“. Nach diesem Erwägungsgrund sind dabei auch der für die „Identifizierung“ zu betreibende Aufwand / die benötigten Ressourcen zu berücksichtigen.

Weil es immer auf die Möglichkeiten des Verantwortlichen oder irgendeines anderen ankommt, einen Personenbezug herzustellen, ist es angesichts der „verdichteten Masse an Daten“ im Gesundheitsbereich und den „neuen Techniken“ wie Big Data und Co. sowie der Mitteilungsbedürftigkeit von Patienten etc. heutzutage mitunter schwierig zu entscheiden, ob Daten noch personenbezogen, pseudonym oder anonym sind.

In diesem Zusammenhang gilt es zu beachten, dass in den Regelungen der DS-GVO der Begriff der Anonymisierung nicht mehr vorkommt. Lediglich in den Erwägungsgründen wird er in ErwGr. 26 erwähnt.

6.2. Gesundheitsdaten

Kommentar:

Gesundheitsdaten werden nach der Verordnung als personenbezogene Daten definiert, „*die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen*“. Die Verordnung verwendet mithin eine ziemlich weite Definition der Gesundheitsdaten.

Diesbezüglich empfiehlt es sich, ergänzend auch den Erwägungsgrund 35 einzubeziehen. Dieser führt weitere Bereiche auf, in denen Gesundheitsdaten verarbeitet werden. So gilt gemäß dieses Erwägungsgrunds „*zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen. Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen im Sinne der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates für die natürliche Person erhoben werden, Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren, Informationen, die von der Prüfung oder Untersuchung eines Körperteils oder einer körpereigenen Substanz, auch aus genetischen Daten und biologischen Proben, abgeleitet wurden, und Informationen etwa über Krankheiten, Behinderungen, Krankheitsrisiken, Vorerkrankungen, klinische Behandlungen oder den physiologischen oder biomedizinischen Zustand der betroffenen Person unabhängig von der Herkunft der Daten, ob sie nun von einem Arzt oder sonstigem Angehörigen eines Gesundheitsberufes, einem Krankenhaus, einem Medizinprodukt oder einem In-vitro-Diagnostikum stammen.*“

Zusammenfassend lässt sich deshalb feststellen, dass der Definition der DS-GVO folgend, sehr viele Daten, denen man unmittelbar keinen Gesundheitsbezug ansehen würde, aufgrund der Möglichkeit der Kombination mit anderen Daten, schnell einen Gesundheitsbezug „erben“ können.

6.3. Genetische Daten

Kommentar:

Art. 4 Abs. 13 führt aus: genetische Daten sind „personenbezogene Daten

- zu den ererbten oder erworbenen genetischen Eigenschaften
- einer natürlichen Person,
- die eindeutige Informationen über die Physiologie oder
- die Gesundheit dieser natürlichen Person liefern und
- insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden“.

D. h. unter genetische Daten werden alle Arten von Informationsträgern erfasst, die ererbte oder erworbene genetische Informationen zu einer natürlichen Person enthalten und aus denen Informationen bzgl. Physiologie und/oder Gesundheit gewonnen werden können.

Damit umfasst der Begriff der genetischen Daten natürlich neben den „klassischen“ Proben einer Biomaterialbank auch andere Materialien, die innerhalb der Gesundheitsversorgung von einem Patienten gewonnen werden wie beispielsweise Blutproben.

Die Artikel-29-Datenschutzgruppe äußerte sich zu diesem Thema bereits 2004 in WP 91[4] und bezog bei der Interpretation auch die Definition der UNESCO[5] mit ein. Zu den aus dem Material gewinnbaren Informationen, die bei der Beurteilung „genetisches Datum ja/nein“, berücksichtigt werden müssen, zählen demnach insbesondere

- Biologische Abstammung
- Krankheitsdispositionen
- Informationen über gewisse Besonderheiten /Fähigkeiten
- Informationen über Lebensumstände.

Diese Art von Informationen behalten zudem über lange Zeiträume ihre Gültigkeit und ermöglichen sogar Aussagen über zukünftige Entwicklungen. Weiterhin können die darin implizit enthaltenen Informationen eine Bedeutung von erheblicher Tragweite für das Leben des Betroffenen sowie naher Anverwandter beinhalten. Eine Speicherung und spätere Auswertung genetischer Daten kann sogar heute noch ungeborene Personen berühren. Z. B. wenn aufgrund der heute gewonnenen genetischen Daten einer Person in 60 Jahren bei einem Enkel der Person eine (heute evtl. noch unbekannte) Erkrankung offenbart wird, die zur Stigmatisierung und Ausgrenzung führt. Daher beinhalten genetische Daten oftmals nicht nur Informationen zu einer Person und es stellt sich immer die Frage, in wieweit eine Person bei einer Einwilligung bzgl. der Verarbeitung genetischer Daten auch für andere betroffene Personen (Eltern, Kinder, Geschwister, ...) einwilligen kann.

6.4. Verarbeitung

Kommentar:

Der Begriff der „Verarbeitung“ erfasst als Oberbegriff alle Arten des „Datenumgangs“. So erfasst er:

- *das Erheben,*
- *das Erfassen,*
- *die Organisation,*
- *das Ordnen,*
- *die Speicherung,*
- *die Anpassung oder Veränderung,*
- *das Auslesen,*
- *das Abfragen,*
- *die Verwendung,*
- *die Offenlegung durch Übermittlung,*
- *die Verbreitung oder eine andere Form der Bereitstellung,*
- *den Abgleich oder die Verknüpfung,*
- *die Einschränkung* (in Deutschland auch bekannt als „Sperrung“)*,*
- *das Löschen oder etwa die Vernichtung*.

Es fällt diesbezüglich auf, dass für viele der in der DS-GVO verwendeten Begrifflichkeiten keine weiteren Definitionen existieren, sodass man nur mutmaßen kann, was der Gesetzgeber damit

[4] Artikel-29-Datenschutzgruppe (2004) Arbeitspapier über genetische Daten. Online, zitiert am 2016-04-22; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp91_de.pdf

[5] United Nations Educational, Scientific and Cultural Organization (2003) International Declaration on Human Genetic Data. Online, zitiert am 2016-04-22; Verfügbar unter http://unesdoc.unesco.org/images/0013/001331/133171e.pdf#page=45

eigentlich meint. Um etwaigen Schwierigkeiten bei der Definition aus dem Wege zu gehen, empfiehlt es sich deshalb bei Unklarheiten den Oberbegriff „Verarbeitung“ zu nutzen.

6.5. Für die Verarbeitung Verantwortlicher

Kommentar:

Der „Verantwortliche“ wird von der Verordnung definiert als *„die „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet*“.

Die Bestimmung der Verantwortlichkeit ist maßgeblich für die nach der DS-GVO zu erfüllenden Pflichten. Aus diesem Grund ist es erforderlich, gerade bei Sachverhalten, in denen viele Beteiligte eine gewisse Rolle bei der Datenverarbeitung spielen, zu entscheiden, wer eigentlich für welche Datenverarbeitung die Verantwortung trägt.

Dazu ist es entscheidend, abzugrenzen, wer von den jeweils Beteiligten im jeweiligen Einzelsachverhalt über die Mittel und Zwecke der Datenverarbeitung entscheidet. Gerade bei Datenverarbeitungen, die ausgelagert (z. B. in einer „Cloud“ eines externen Anbieters) erfolgen, ist dies nicht immer trivial, aber dennoch zwingend erforderlich.

Grundsätzlich macht es dem Gesetzeswortlaut der Verordnung nach zunächst keinen Unterschied, ob es sich um einen öffentlichen oder privaten Verantwortlichen handelt. Für beide gilt prinzipiell gleiches Recht und deshalb müssen sie grundsätzlich auch die gleichen Pflichten / Anforderungen erfüllen.

Da Behörden jedoch meistens im öffentlichen Auftrag tätig werden, existieren für die Verarbeitung durch Behörden im öffentlichen Interesse einige Regelungen, die nationale Öffnungsklauseln enthalten bzw. der jeweiligen Datenverarbeitung eine gesetzliche Legitimierung verschaffen.

6.6. Datei / Dateisystem:

Kommentar:

Bemerkenswert ist, dass die DS-GVO auch weiterhin den u.a. in Deutschland in Bereichen des Landesdatenschutzrechts, d. h. für den öffentlichen Bereich, verbreiteten Dateibegriff weiterhin verwendet bzw. aufgreift. U.a. daran lässt sich der Ansatz der Verordnung erkennen, sich eher „technologieneutral“ zu positionieren, um auf technische Neuerungen vorbereitet zu sein und solche Sachverhalte durch die in der DS-GVO enthaltenen Regelungen entsprechend angemessen lösen zu können. Ferner lässt sich an diesem Begriff auch die neuartige „Risikoausrichtung“ der DS-GVO erkennen, denn auch von Dateien kann, wie uns die Vergangenheit gezeigt hat, ein nicht unbeträchtliches Risiko für Betroffene ausgehen, weshalb es nur konsequent ist, den Dateibegriff im Regelungsumfeld zu nutzen. Die DS-GVO findet deshalb sowohl auf digitale als auch „analoge“ „Dateisysteme“ Anwendung.

Dateisystem ist „jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird“.

Damit werden durch die Regelungen der DS-GVO auch Papierlisten, auf denen Patientendaten nach bestimmten Kriterien geordnet sind, erfasst.

6.7. Pseudonymisierung

Kommentar:

Art. 4 Abs. 5 definiert Pseudonymisierung als „die Verarbeitung personenbezogener Daten in einer Weise, dass

- die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können,
- sofern diese zusätzlichen Informationen gesondert aufbewahrt werden
- und technischen und organisatorischen Maßnahmen unterliegen,
- die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

Allein aus der Begriffsbestimmung lassen sich verschiedene implizite enthaltene Vorgaben ableiten:

a) Pseudonyme Daten stellen gemäß Art. 4 Abs. 1 personenbezogene Daten dar, da eine grundsätzliche Möglichkeit zur Identifikation der Person besteht.
b) Der Vorgang der Pseudonymisierung stellt eine Verarbeitung im Sinne von Art. 4 Abs. 2 dar, somit gelten für eine Pseudonymisierung alle Vorgaben bzgl. der Verarbeitung, insbesondere die Vorgaben von Art. 5 und Art. 6 bzw. Art. 9. D. h. auch bei einer Pseudonymisierung muss die Rechtmäßigkeit der Verarbeitung gewährleistet sein. Insbesondere muss bei der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 ein Erlaubnistatbestand zur Pseudonymisierung vorhanden sein.
c) Pseudonyme Daten gelten nur als pseudonym, wenn der die Daten Verarbeitende keine Möglichkeit hat, die Zuordnungsvorschrift zwischen Pseudonym und Personenkennung zu verarbeiten.

Grundsätzlich muss zudem festgehalten werden, dass eine Pseudonymisierung keine Anonymisierungstechnik darstellt, wie die Artikel-29-Datenschutzgruppe in WP 216[6] feststellte: eine Pseudonymisierung „verringert lediglich die Verknüpfbarkeit eines Datenbestands mit der wahren Identität einer betroffenen Person und stellt somit eine sinnvolle Sicherheitsmaßnahme dar“[6]. Insbesondere sind pseudonymisierte Daten nicht mit anonymisierten Informationen gleichzusetzen[6].

6.8. Empfänger, Dritte und Unternehmen

6.8.1. Empfänger

Kommentar:

Entsprechend Art. 4 Abs. 9 DS-GVO ist ein Empfänger eine „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden“. Der Begriff des Empfängers ist dabei vom Begriff des Dritten losgelöst, d. h. Empfänger ist sowohl ein Auftragsverarbeiter als auch jeder Dritte.

Einzige Ausnahme: Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten personenbezogene Daten erhalten, gelten nicht als Empfänger (siehe auch ErwGr. 31).

[6] Artikel-29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken. Online, zitiert am 2016-04-22; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

6.8.2. Dritte

Kommentar:

Art. 4 Abs. 10 DS-GVO definiert Dritte als „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle“, außer

- der betroffenen Person,
- dem Verantwortlichen,
- dem Auftragsverarbeiter und
- den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

6.8.3. Unternehmen

Kommentar:

Art. 4 Abs. 18 DS-GVO definiert ein Unternehmen als „eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen“. Entsprechend ErwGr. 150 ist der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102[7] des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) zu verstehen. Damit gilt der kartellrechtliche Unternehmensbegriff. Ob eine Tätigkeit tatsächlich im Wettbewerb erbracht wird, ist dabei unerheblich. Maßgeblich ist das Ergebnis im hypothetischen Wettbewerbstest: findet ein Wettbewerb statt?

In der Vergangenheit gab es immer wieder Schwierigkeiten in der Anwendung des funktionalen Unternehmensbegriffs innerhalb der öffentlichen Verwaltung. Kann der Unternehmensbegriff zutreffen, wenn der Staat keinen Wettbewerb eröffnet und die Beziehungen zwischen Staat und Nutzern rein öffentlich-rechtlich ausgestaltet sind? Entsprechend Unionsrecht sind hoheitliche bzw. nicht-wirtschaftliche Aufgaben nur jene Aufgaben, die wesensgemäß mit der Ausübung von Hoheitsrechten verbunden sind. D. h. es ist bei der Beurteilung, ob es sich um ein Unternehmen handelt oder nicht, unerheblich, ob eine öffentlich-rechtliche Ausgestaltung vorliegt, sondern es muss ausschließlich bewertet werden, ob die Aufgabe vom Wesen her eine hoheitliche Aufgabe darstellt[8]: „Ein Unternehmen ist jede eine wirtschaftlich Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung“[9]. Für den Gesundheitsbereich sind damit Krankenhäuser, Arztpraxen, Apotheken usw. als Unternehmen anzusehen.

In der Definition des EuGH bzgl. des Unternehmensbegriffs ist die „wirtschaftliche Einheit“ enthalten, wobei die wirtschaftliche Einheit dabei nicht nur aus einem einzelnem Unternehmen, sondern auch aus mehreren natürlichen und juristischen Personen bestehen kann[9]. Damit verbunden ist ggfs. eine gemeinschaftliche Haftung für Verstöße innerhalb eines Unternehmens, d. h. unter Umständen muss eine Muttergesellschaft für eine Tochter haften. Im Unternehmensbegriff des EuGH sind die

[7] Vertrag über die Arbeitsweise der Europäischen Union, Dritter Teil - Die internen Politiken und Maßnahmen der Union, Titel VII - Gemeinsame Regeln betreffend Wettbewerb, Steuerfragen und Angleichung der Rechtsvorschriften, Kapitel 1 – Wettbewerbsregeln, Abschnitt 1 - Vorschriften für Unternehmen: Artt. 101, 102. Online, zitiert am 2016-05-19; Verfügbar unter https://dejure.org/gesetze/AEUV/101.html bzw. https://dejure.org/gesetze/AEUV/102.html

[8] EuG Urt. v. 16.07.2014 Az.: T-309/12. Online, zitiert am 2016-05-19; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=EuG&Datum=16.07.2014&Aktenzeichen=T-309/12

[9] Faust S, Spittka J, Wybitul T (2016) Milliardenbußgelder nach der DS-GVO? Ein Überblick über die Sanktionen bei Verstößen gegen den Datenschutz. ZD: 120 - 125

natürlichen Personen jedoch ebenso beinhaltet, sodass die Handlungen irgendeiner natürlichen Person, die für das betreffende Unternehmen handelt, immer dem Unternehmen zuzurechnen sind. Diese Haftung des Unternehmens für die Handlungen natürlicher Personen ist nur dort begrenzt, wo „die Person die Grenzen ihrer Funktionen überschreitet“[9] und diese Überschreitung auch aus anderen Gründen dem Unternehmen nicht zuzurechnen ist.

6.9. Öffentliches Interesse i. V. m. öffentlicher Gesundheit

Kommentar:

Erwägungsgrund 54 referenziert bzgl. des Begriffes „öffentliche Gesundheit“ Verordnung (EG) Nr. 1332/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 über Lebensmittelenzyme und zur Änderung der Richtlinie 83/417/EWG des Rates, der Verordnung (EG) Nr. 1493/1999 des Rates, der Richtlinie 2000/13/EG, der Richtlinie 2001/112/EG des Rates sowie der Verordnung (EG) Nr. 258/97.

In dieser Verordnung wird der Begriff der öffentlichen Gesundheit hinsichtlich Gemeinschaftsstatistiken über öffentliche Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz verwendet. Der Begriff selbst umfasst dabei eine weites Feld: „alle Elemente im Zusammenhang mit der Gesundheit wie Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von und den allgemeinen Zugang zu Gesundheitsversorgungsleistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen“ (Erwägungsgrund 54).

Grundsätzlich beachtet werden muss hierbei, dass eine Verarbeitung aufgrund von öffentlichem Interesse auch nur von Institutionen durchgeführt werden darf, die im (nationalen) öffentlichen Interesse handeln, also den direkten Auftrag vom nationalen Gesetzgeber bekamen. Erwägungsgrund 54 schreibt hierzu: „Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber, Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten“.

6.10. Verhältnismäßigkeit einer Maßnahme

Kommentar:

Damit eine Maßnahme, die in Grundrechte eingreift, nicht rechtswidrig ist, muss sie dem kompletten Begriff der Verhältnismäßigkeit genügen. (Ableitbar Art. 20 Abs. 3 Grundgesetz, siehe auch ständige Rechtsprechung des BVerfG z. B.) Dazu muss eine Maßnahme

a) einen legitimen Zweck verfolgen,
b) geeignet und erforderlich sein
c) sowie angemessen sein.

Eingriffe in die informationelle Selbstbestimmung eines Betroffenen entsprechen immer einem Grundrechtseingriff, sodass hier eine Prüfung der Verhältnismäßigkeit unabdingbar ist.

Wird die Frage nach der Legitimität der Maßnahme bereits verneint, erübrigt sich die Prüfung der anderen Anforderungen: nur wenn die Legitimität gewährleistet ist, kann die Verhältnismäßigkeit erfüllt werden.

6.10.1. Legitimer Zweck

Kommentar:

Ein Zweck ist dann legitim, wenn er als solcher verfolgt werden darf. Im gesetzgeberischen Umfeld folgt daraus, dass der Zweck auf das Wohl der Allgemeinheit gerichtet sein muss. Allgemein folgt daraus:

a) Der Zweck bzw. das daraus resultierende Ziel darf nicht durch ein Gesetz verboten sein.
b) Ist der Zweck weder erlaubt noch verboten, es werden aber Rechte anderer eingeschränkt, so muss der Zweck bzw. das aus dem Zweck resultierende Ziel dem Wohl der Allgemeinheit nützen.

6.10.2. Geeignetheit einer Maßnahme

Kommentar:

Eine Maßnahme ist dann geeignet, wenn mit ihrer Hilfe das angestrebte Ziel gefördert bzw. erreicht werden kann. Dabei wird ausschließlich die Zwecktauglichkeit der Maßnahme beurteilt, nicht deren Effektivität. Zur Beurteilung ist daher folgende Frage zu beantworten:

– Bewirkt (oder fördert) die Maßnahme das Erreichen des Zwecks?

6.10.3. Erforderlichkeit einer Maßnahme

Kommentar:

In der DS-GVO selbst wird der Begriff der „Erforderlichkeit“ bzw. „Notwendigkeit“ nicht definiert. Allerdings finden sich in den Erwägungsgründen Kriterien, welche die Beurteilung der Erforderlichkeit erleichtern. Daten sind insbesondere dann erforderlich oder notwendig, wenn

- der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (Erwägungsgrund 39) oder
- der Zweck der Verarbeitung nicht im lebenswichtigen Interesse der betroffenen Person liegt (Erwägungsgrund 112).

D. h. damit eine Maßnahme erforderlich ist, darf es kein milderes (= in die Rechte Betroffener weniger eingreifendes) Mittel geben, welches den gleichen Erfolg mit vergleichbarem Aufwand erzielt. Um die Erforderlichkeit / Notwendigkeit beurteilen zu können, müssen daher drei Fragen beantwortet werden:

1) Gibt es ein anderes Mittel?
2) Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen?
3) Ist dieses Mittel ein milderes, also die Rechte Anderer weniger belastendes Mittel?

6.10.4. Angemessenheit einer Maßnahme

Kommentar:

Eine Maßnahme muss „angemessen“ sein. D. h. die (Eingriffs-) Intensität einer Maßnahme in die Rechte Anderer muss

a) in einem angemessenen Verhältnis zur Bedeutung und Dringlichkeit des Ziels stehen und
b) die Grenze der Zumutbarkeit gewahrt bleiben.

Letztlich ist somit eine Abwägung zwischen den betroffenen Interessen notwendig:

– Wie bedeutsam ist das Ziel für die Allgemeinheit? Welchen (substanziellen) Vorteil hat die Allgemeinheit bei Erreichung des Zieles?

- Welcher Nachteil entsteht den Betroffenen?
- Welches Ziel verfolgt der Datenverarbeitende? Welcher Vorteil soll erlangt werden?
- Erfolgt die Maßnahme zur Förderung oder zum Schutz von Rechtsgütern? Oder dient die Maßnahme ausschließlich oder überwiegend wirtschaftlichen Vorteilen?
- Wie ist der Rang des geförderten/geschützten Rechtsgutes im Verhältnis zu den eingeschränkten Rechtsgütern der Betroffenen?
- Wie stehen die Vorteile der Maßnahme im Zusammenhang mit deren Nachteilen?

Dabei gilt: je intensiver die Maßnahme in die Grundrechte von Betroffenen eingreift, umso höhere Anforderungen sind an die Dringlichkeit des Zieles zu stellen.

Dabei sind insbesondere die folgenden Abwägungsfehler zu vermeiden:

- Abwägungsdefizit: nicht alle abwägungsrelevanten Belange werden ermittelt und berücksichtigt
- Abwägungsüberschreitung: es werden planfremde Ziele oder Belange herangezogen
- Abwägungsfehleinschätzung: die Gewichtigkeit der Belange werden falsch eingeschätzt
- Abwägungsdisproportionalität: zwischen widerstreitenden Belangen wird kein angemessener Ausgleich hergestellt.

6.10.5. Interessenabwägung

Kommentar:

Der BGH konkretisierte die erforderliche Abwägung in seinem Urteil vom 17.12.1985 (Az. VI ZR 244/84)[10]: es erfolgt eine Abwägung des Persönlichkeitsrechts des Betroffenen und des Stellenwerts, den die Offenlegung und Verwendung der Daten für den oder die Betroffenen hat, gegen die Interessen der speichernden Stelle und der Dritten, für deren Zweck die Speicherung erfolgte. „Dabei sind Art, Inhalt und Aussagekraft der beanstandeten Daten an den Aufgaben und Zwecken zu messen, denen ihre Speicherung dient[11].“ Die Abwägung ist dabei für jede Art der Datenverarbeitung (Erhebung, Speicherung, Übermittlung, ...) getrennt zu prüfen. Dabei kann es auch vorkommen, dass eine Abwägung, der zufolge eine Erhebung und Speicherung statthaft ist, eine Übermittlung jedoch nicht legitimiert.

Grundsätzlich kommen als schutzwürdige Interessen der Betroffenen „alle menschlichen Ziele in Betracht, das Streben nach Geld, Anerkennung, nach Privatheit wie nach Kommunikation“, ebenso „das Streben nach Glück“[12]. Dabei gilt, dass die Interessen der Betroffenen als umso schutzwürdiger anzusehen sind,

- je sensitiver die Daten sind und
- je größer die Zahl der die Daten verarbeitenden Personen bzw., bei Übermittlungen, der Abrufberechtigten ist[12].

[10] Bundesgerichtshof Urt. v. 17.12.1985, Az.: VI ZR 244/84 Online, zitiert am 2016-04-22; Verfügbar unter (http://dejure.org/dienste/vernetzung/rechtsprechung?Text=NJW%201986,%202505)

[11] Bundesgerichtshof Urt. v. 17.12.1985, Az.: VI ZR 244/84, Rn. 13 Online, zitiert am 2016-04-22; Verfügbar unter https://www.jurion.de/Urteile/BGH/1985-12-17/VI-ZR-244_84

[12] BeckOK DatenSR/von Lewinski BDSG § 10 Rn. 23-29

Bei der Darstellung der Betroffeneninteressen kann die Sphärentheorie[13,14] und ihre Einteilung in die drei Sphären Intim-, Privat- und Sozialsphäre helfen:

- ein Eingriff in die Intimsphäre muss vermieden werden, da hier der Kern der Menschenwürde betroffen ist
- Privat- und Sozialsphäre: hier gilt, je stärker der Eingriff, desto gewichtiger muss das verfolgte Gemeinwohlinteresse (= Verarbeitungszweck) sein.

[13] BeckOK DatenSR/Wolff BDSG § 28 Rn. 64-70

[14] BVerfG Urt. v. 31.01.1973, AZ.: 2 BvR 454/71 Online, zitiert am 2016-04-22; Verfügbar unter http://dejure.org/dienste/vernetzung/rechtsprechung?Text=BVerfGE%2034,%20238; BGH Urt. v. 27.01.2010 Az.: IV ZR 129/09 Online, zitiert am 2016-04-22; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=27.01.2010&Aktenzeichen=IV%20ZR%20129/09

7. Rechtsgrundlage für Verarbeitung von Gesundheitsdaten

Kommentar:

Auch wenn um das „Verbot mit Erlaubnisvorbehalt“ innerhalb der Kompromissfindung stark gestritten wurde, so findet sich das Prinzip letztlich doch in Artikel 6 „Rechtmäßigkeit der Verarbeitung“ als auch in Artikel 9 „Verarbeitung besonderer Kategorien personenbezogener Daten“ der DS-GVO wieder: Datenverarbeitungsvorgänge sind nur zulässig, wenn die Person zugestimmt hat oder die Datenverarbeitung zu einer Vertragserfüllung erforderlich ist oder eine andere in der jeweiligen Vorschrift genannte Ausnahme die Verarbeitung gestattet.

7.1. Rahmenbedingungen für die Verarbeitung personenbezogener Daten

Fundstelle in der DS-GVO:

– Art. 5 „Grundsätze für die Verarbeitung personenbezogener Daten“

Kommentar:

Eine Datenverarbeitung muss gemäß den Vorgaben der DS-GVO folgende Grundsätze berücksichtigen:

1) Treu und Glauben
2) Zweckbindung
3) Datenminimierung
4) Richtigkeit
5) Speicherbegrenzung
6) Integrität und Vertraulichkeit
7) Rechenschaftspflicht

7.1.1. Treu und Glauben

Kommentar:

Treu und Glauben ist ein unbestimmter Rechtsbegriff und bezeichnet das Verhalten eines redlich und anständig handelnden Menschen. In Art. 5 Abs. a Lit. a wird verlangt, dass die Verarbeitung personenbezogener Daten auf eine rechtmäßige und in einer für die betroffene Person nachvollziehbaren Weise erfolgt. Dies beinhaltet also eine Forderung nach einer Rechtmäßigkeit und Transparenz der Verarbeitung, geht also über den allgemeinen „Treu und Glauben“ Begriff hinaus.

7.1.2. Zweckbindung und zweckkompatible Verarbeitung

Kommentar:

Art. 5 Abs. 1 Lit. b DS-GVO verlangt, dass personenbezogene Daten für „festgelegte, eindeutige und legitime Zwecke“ (Zweckbindung) erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. D. h. Daten dürfen prinzipiell zu anderen Zwecken verarbeitet werden (Zweckänderung), wenn diese neuen Zwecke mit den Zwecken, zu welchen die Daten ursprünglich erhoben wurden, vereinbar sind.

Eine Weiterverarbeitung für „im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke“ gilt nicht als unvereinbar mit den ursprünglichen Zwecken (Art. 5 Abs. 1 Lit. b DS-GVO). Natürlich muss auch hier der Forschungs- oder Archivzweck im angemessenen Verhältnis zum ursprünglichen Zweck stehen.

Art. 6 Abs. 4 DS-GVO erlaubt eine „zweckkompatible“ Verarbeitung, ohne zu nennen, wann eine Kompatibilität gegeben sein soll. Es werden zwar Erwägungsaspekte (z. B. ob die beiden Zwecke miteinander in einer Verbindung stehen) genannt, eine Folge für die Zulässigkeit der Verarbeitung wird daraus jedoch nicht abgeleitet.

Bei der Beurteilung bzgl. „Zweckkompatibilität“ sollen insbesondere die folgenden Faktoren berücksichtigt werden:

- eine Verbindung zwischen den Zwecken (Art. 6 Abs. 4 Lit. a DS-GVO)
- der Gesamtkontext, in dem die Daten erhoben wurden (Art. 6 Abs. 4 Lit. b DS-GVO)
- die Art der personenbezogenen Daten (Art. 6 Abs.4 Lit. c DS-GVO)
- die möglichen Konsequenzen für den Betroffenen (Art. 6 Abs. 4 Lit. d DS-GVO) und
- das Vorhandensein von angemessenen Sicherheitsmaßnahmen (Art. 6 Abs. 4 Lit. e DS-GVO), wozu eine Verschlüsselung oder Pseudonymisierung der Daten gehören kann.

Allerdings stellt Art. 6 DS-GVO keinen Erlaubnistatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten dar, da Art. 9 Abs. 1 DS-GVO die Verarbeitung grundsätzlich verbietet, außer einer der in Art. 9 DS-GVO genannten Erlaubnistatbestände gestattet die Verarbeitung besonderer Kategorien personenbezogener Daten. Damit ist Art. 6 insbesondere auch kein Erlaubnistatbestand zur Verarbeitung von Gesundheitsdaten.

Damit ist eine zweckkompatible Verarbeitung von Daten der besonderen Kategorien basierend auf den Vorgaben von Art. 6 DS-GVO nicht möglich.

7.1.3. Datenminimierung

Kommentar:

Art. 5 Abs. 1 Lit. c DS-GVO verlangt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ müssen. D. h. hier ist eine (vom Betroffenen und Aufsichtsbehörden nachvollziehbare) Abwägung erforderlich, welche Daten für die angestrebten Ziele angemessen und notwendig sind. Dabei ist „notwendig“ im Sinne von „objektiv erforderlich“ zu interpretieren.

Bzgl. Angemessenheit siehe Kapitel 6.10.4, bzgl. Erforderlichkeit Kapitel 6.10.3

7.1.4. Richtigkeit

Kommentar:

Entsprechend Art. 5 Abs.1 Lit. d DS-GVO müssen personenbezogene Daten „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein“. D. h. der Verantwortliche hat „alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden“.

Bzgl. Angemessenheit siehe Kapitel 6.10.4

7.1.5. Speicherbegrenzung

Kommentar:

Personenbezogene Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“. D. h. Art. 5 DS-GVO beinhaltet im Gegensatz zum BDSG kein absolutes Löschgebot, sondern Daten dürfen weiterhin gespeichert werden, wenn die Identifizierung der betroffenen Daten unmöglich ist. Dabei muss hierbei eine Re-Identifikation nachweislich ausgeschlossen sein.

Für im „öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke“ dürfen personenbezogene Daten länger gespeichert werden, sofern den Vorgaben der DS-GVO (z. B. Stand der Technik) genügende geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten vor unbefugtem Zugriff getroffen wurden.

7.1.6. Integrität und Vertraulichkeit

Kommentar:

Weiterhin müssen personenbezogene Daten in einer Weise verarbeitet werden, die eine „angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“ (Art. 5 Abs. 1 Lit. f DS-GVO). Das Bundesverfassungsgericht urteilte 2008 bereits, dass die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein Grundrecht darstellt[15], sodass diese Anforderungen letztlich keine Neuerungen in Deutschland darstellen.

7.1.7. Rechenschaftspflicht

Kommentar:

Personenbezogene Daten müssen in einer Weise verarbeitet werden, dass der Verantwortliche nachweisen kann, dass alle aus Art. 5 Abs. 1 DS-GVO resultierenden Anforderungen erfüllt wurden (Art. 5 Abs. 2 DS-GVO). D. h. hier wird eine Dokumentationspflicht verankert, welche folgenden Kriterien genügen muss:

- Vollständige, ordnungsgemäße Dokumentation des Verfahrens
- Nachvollziehbarkeit der Dokumentation
- Schutz vor Veränderung und Verfälschung
- Sicherung vor Verlust
- Prüfbarkeit
- Einhaltung einer dem Verfahren genügenden Aufbewahrungsfrist.

Letztlich wird also eine revisionssichere datenschutzrechtliche Dokumentation erforderlich sein, damit der Verantwortliche seiner aus Art. 5 Abs. 2 resultierenden Rechenschaftspflicht genügt.

7.1.8. Verarbeitung durch Fachpersonal

Kommentar:

Art. 9 Abs. 3 DS-GVO schreibt vor, dass „Daten von Fachpersonal oder unter dessen Verantwortung“ verarbeitet werden müssen, der Terminus „Fachpersonal“ wird durch die DS-GVO jedoch nicht definiert. Das Fachpersonal muss jedoch „nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis“ unterliegen. Somit muss das Fachpersonal zur Gruppe der Geheimnisträger entsprechend §203 StGB gehören, dies sind im medizinischen Umfeld i. A. die in §203 Abs. 1 Ziff. 1 StGB genannten Personenkreise:

[15] BVerfG Urt. v. 27. Februar 2008, Az. : 1 BvR 370/07. Online, zitiert am 2016-05-12; Verfügbar unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

- Arzt,
- Zahnarzt,
- Tierarzt,
- Apotheker
- Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert.

Entsprechend §203 Abs. 3 S. 2 StGB stehen dem Geheimnisträger „ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind“. Dementsprechend muss das Fachpersonal dem Personenkreis von §203 Abs. 1 Ziff. 1 und Abs. 3 S.2 StGB angehören.

7.2. Einwilligung

7.2.1. Einwilligung Erwachsene

Fundstelle in der DS-GVO:

- Art. 7 „Bedingungen für die Einwilligung“

Kommentar:

Gegenüber den Regelungen der Datenschutzrichtlinie wurden die formalen Anforderungen an eine wirksame Einwilligung präzisiert (Erwägungsgründe 25, 32 und 34): Die Einwilligungserklärung muss „freiwillig, spezifisch, informiert und eindeutig” (siehe auch die Begriffsbestimmung in Art. 4 Abs. 11) sein. Stillschweigendes Einverständnis, standardmäßig angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten daher keine Einwilligung darstellen. (Erwägungsgrund 25). Auch Inhalte einer Einwilligungserklärung wie die Angabe des für die Verarbeitung Verantwortlichen wie auch die Datenverarbeitungszwecke werden vorgegeben (Erwägungsgrund 32).

In Art. 7 werden die Voraussetzungen für die Einwilligung beschrieben. Dazu zählen insbesondere:

- Bei Einholung Einwilligung in Zusammenhang mit anderen Sachverhalten: „verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist“ (Art. 7. Abs. 2) (= ist für den Betroffenen transparent dargestellt, worum es geht und welche Auswirkungen es hat oder haben könnte“)
- Recht zum Widerruf, Hinweis auf das Recht bei Einwilligung (Art. 7 Abs. 3)
- Hinweis, dass Widerruf die Rechtmäßigkeit der erfolgten Datenverarbeitung bis Erteilung des Widerrufs nicht berührt (Art. 7 Abs. 3)
- Widerruf mindestens so einfach abzugeben wie die Einwilligung
- Kopplungsverbot der Einwilligung mit Vertragsabschluss, Erbringung Dienstleistung o.ä.

Bei der Interpretation der rechtlichen Vorgaben bzgl. der Einwilligung sind natürlich ergänzend die Erwägungsgründe des europäischen Gesetzgebers zu beachten, insbesondere:

- Erwägungsgrund 32 (Grundlegende Anforderungen)
- Erwägungsgrund 33 (Forschung)
- Erwägungsgrund 38 (Einwilligung Kind)
- Erwägungsgrund 40 (Rechtmäßigkeit der Verarbeitung)
- Erwägungsgrund 42 (Nachweispflicht)
- Erwägungsgrund 43 (Freiwilligkeit)
- Erwägungsgrund 50 (Zweckänderung)

- Erwägungsgrund 51 (Besondere Kategorien von Daten)
- Erwägungsgrund 54 (öffentliches Interesse)
- Erwägungsgrund 111 (Datenübermittlung)
- Erwägungsgrund 155 (Beschäftigtenkontext)
- Erwägungsgrund 161 (Forschung)

So erfolgt in Erwägungsgrund 34 eine Einschränkung der Einwilligung bzgl. der Rechtsgültigkeit, wenn

- zwischen betroffener Person und dem für die Verarbeitung Verantwortlichen ein klares Ungleichgewicht besteht (z. B. Arbeitgeber und Arbeitnehmer),
- wenn zu verschiedenen Datenverarbeitungsvorgängen keine gesonderte Einwilligung eingeholt wird, obwohl dies im Einzelfall angebracht ist, oder
- die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der die Einwilligung abhängig gemacht wird, obwohl dies für diese Erfüllung nicht erforderlich ist.

Die DS-GVO verlangt im Gegensatz zum heutigen BDSG für die Einwilligung keine Schriftform mehr. Grundsätzlich muss der Datenverarbeiter jedoch nachweisen, dass der Betroffene seine Einwilligung rechtskonform gegeben hat (Art. 7 Abs. 1, Erwägungsgrund 32).

Wichtig ist die Beachtung der „Übergangsregelung“ (Erwägungsgrund 171) bzgl. einer Einwilligung:

> „Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, sodass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verordnung fortsetzen kann“.

D. h. heute gegebene Einwilligungen, welche die Vorgaben der DS-GVO berücksichtigen, gelten für die Zukunft. Dieser Umstand kann in der Medizin in verschiedenen Bereichen sehr wichtig sein, z. B. für

- Nachsorge in der Onkologie
- Krankheitsregister, die nicht gesetzlich geregelt sind
- Forschungsvorhaben.

7.2.2. Einwilligung Kind (Dienste der Informationsgesellschaft)

Fundstelle in der DS-GVO:

- Art. 8 „Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft“

Kommentar:

Speziell geregelt wurden auch die Bedingungen für die Zustimmung eines Kindes in Bezug auf die Dienste der Informationsgesellschaft. Kinder sowie Jugendliche unter 16 Jahre müssen die Erlaubnis der Eltern einholen, wenn sie in die Verwendung ihrer Daten einwilligen möchten.

Dabei steht es den Mitgliedsstaaten frei, die Altersgrenze weiter herunterzusetzen. Hierbei darf die Altersgrenze von 13 Jahren jedoch nicht unterschritten werden.

7.3. Gesetzliche Erlaubnistatbestände

Kommentar:

Zusätzlich zur Einwilligung sieht die DS-GVO eine Reihe von Erlaubnistatbeständen hinsichtlich der Verarbeitung besonderer Kategorien von personenbezogenen Daten vor. Diese Erlaubnistatbestände entsprechen weitestgehend den aus der Richtlinie 95/46/EG bekannten Erlaubnistatbeständen. Ebenso wie bei der Richtlinie wird dabei eine Datenverarbeitung immer nur dann legalisiert, wenn die Erforderlichkeit zur Datenverarbeitung gegeben ist.

7.3.1. Gesundheitsversorgung

7.3.1.1. Patientenbehandlung

Kommentar:

Die eigentliche Patientenbehandlung findet eine Legitimierung in Art. 9 Abs. 2 Lit. h DS-GVO in Verbindung mit Art. 9. Abs. 3 DS-GVO:

> „die Verarbeitung ist für ... die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs ... erforderlich“

D. h. Art. 9 Abs. 2 Lit. h DS-GVO gestattet die Verwendung von Daten besonderer Kategorien (genetischen Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung, ...) wenn

1) Unionsrecht dies erlaubt oder
2) der entsprechende Mitgliedsstaat einen rechtlichen Erlaubnistatbestand schuf oder
3) ein Vertrag mit einem „Angehörigen eines Gesundheitsberufs“ vorhanden ist.

Ein Aufnahmevertrag, sei es in einem Krankenhaus oder Rehaklinik oder dergleichen, ist i.d.R. kein Vertrag mit einem Angehörigen eines Gesundheitsberufs, sondern mit einer Institution. Unionsrecht kann bzgl. Gesundheitsversorgung nur sehr eingeschränkt Vorgaben erlassen, somit müssen nationalstaatliche Regelungen die Verarbeitung in diesem Kontext erlauben. Der Behandlungsvertrag zwischen dem Behandelnden und dem Patienten über die (entgeltliche) Durchführung einer medizinischen Behandlung ist ein zivilrechtlicher Vertrag, die entsprechenden vertragstypischen Pflichten stehen in §630a BGB.

7.3.1.2. Abrechnung von Leistungen

Kommentar:

Zur Abrechnung von einem Patienten gegenüber erbrachten Leistungen müssen naturgemäß auch dessen personenbezogene Daten verarbeitet werden. Art. 9 Abs. 2 Lit. f DS-GVO gestattet dies in Verbindung mit Art. 9. Abs. 3 DS-GVO:

> „die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich“.

7.3.2. Arbeitsmedizin

Kommentar:

Arbeitsmedizinische Untersuchungen sind einerseits durch Art. 9 Abs. 2 Lit. b DS-GVO gestattet

> „die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht ... soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist“,

andererseits erhalten sie mit Art. 9 Abs. 2 Lit. h DS-GVO in Verbindung mit Art. 9. Abs. 3 DS-GVO eine Legitimation

> „die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten ... auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs ... erforderlich“.

Damit diese Untersuchungen erlaubt sind, muss zunächst einmal die Erforderlichkeit (siehe Kapitel 6.10.3) der Untersuchung gegeben sein. Nur wenn dies der Fall ist, kann die Verarbeitung spezieller Kategorien von Daten für die arbeitsmedizinische Untersuchung gestattet sein, wenn zumindest eine der angegebenen Vorgaben (EU oder nationales Gesetz, Vertrag) erfüllt ist.

Arbeitsrechtlich ist fraglich, ob ein Beschäftigter für eine vom Gesetzgeber oder Arbeitgeber vorgeschriebene arbeitsmedizinische Untersuchung einen entsprechenden Vertrag mit einem Angehörigen eines Gesundheitsberufs abschließt. Im Rahmen des Unionsrechts können arbeitsrechtliche Vorgaben nur schwer verankert werden, sodass hier nationalstaatliche Regelungen greifen müssen.

In Deutschland existieren verschiedene rechtliche Grundlagen für die arbeitsmedizinischen Untersuchungen:

- Arbeitsschutzgesetz
- Verordnung zur arbeitsmedizinischen Vorsorge
- Bildschirmarbeitsverordnung
- Biostoffverordnung (Umgang mit biologischen Arbeitsstoffen)
- Gefahrstoffverordnung (bei einer Belastung durch Gefahrstoffe)
- Gentechnik-Sicherheitsverordnung
- Lärm- und Vibrations-Arbeitsschutzverordnung
- Röntgenverordnung
- Strahlenschutzverordnung
- Unfallverhütungsvorschrift(en) der jeweiligen Berufsgenossenschaft.

Das deutsche Recht unterscheidet dabei *Pflichtuntersuchungen*, welche der Arbeitgeber anbieten und der Beschäftigte annehmen muss, *Angebotsuntersuchungen*, welche der Arbeitgeber anbieten muss und der Beschäftigte annehmen kann sowie *Wunschuntersuchungen*. Bei Letzteren muss entsprechend den Vorgaben aus dem Arbeitsschutzgesetz Beschäftigten die Möglichkeit geboten werden, sich auf eigenen Wunsch im Hinblick auf eine gesundheitliche Belastung bei der Arbeit fachärztlich untersuchen zu lassen.

7.3.3. Nutzung der Daten zur Geltendmachung von Rechtsansprüchen

Siehe Kapitel 7.3.1.2

7.3.4. Gesetzliche Krankheitsregister

Kommentar:

Gesetzlich geregelte Krankheitsregister (z. B. Krebsregister) können einen Erlaubnistatbestand zur Verarbeitung personenbezogener Daten in Art. 9. Abs. 2 Lit. h DS-GVO in Verbindung mit Art. 9. Abs. 3 DS-GVO finden:

> „die Verarbeitung ist für ... für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs ... erforderlich“.

D. h. jedes Gesetz muss den Nachweis der Erforderlichkeit (siehe Kapitel 6.10.3) führen, damit ein entsprechendes Erkrankungs- oder Krankheitsregister (= System/Dienst) personenbezogene Daten verarbeiten darf.

7.3.5. Gesetzliche Qualitätssicherung, öffentliche Gesundheit

Kommentar:

Die gesetzliche Qualitätssicherung (z. B. §§137, 137a SGB V) wie auch die Regelungen zur öffentlichen Gesundheitsvorsorge (Gesundheitsämter, Impfungen in Schule usw. durch Ämter) können einen Legitimationstatbestand in Art. 9. Abs. 2 Lit. i DS-GVO finden:

> „die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich“.

Neben der Erforderlichkeit müssend die entsprechenden Gesetze insbesondere „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses“ vorsehen, damit sie statthaft sind. Dies schließt die Regelungen der DS-GVO mit ein, sodass deutsche Gesetze zur medizinischen Qualitätssicherung bzgl. der Einhaltung dieser Unionsvorgaben geprüft werden müssen.

7.3.6. Öffentliche Archive, Gesundheitsstatistik

Kommentar:

Die Archivgesetze des Bundes und der Länder sehen vor, dass bei Bedarf (z. B. bei Personen der Zeitgeschichte) personenbezogene Daten in ein Bundesarchiv bzw. das jeweilig zuständige Landesarchiv überführt werden. Dieses Vorgehen kann in Art. 9 Abs. 2 Lit. j DSGVO in Verbindung mit Art. 89 Abs. 1 DS-GVO eine Legitimierung finden, Gleiches gilt für die Gesundheitsstatistik des Bundes und der Länder:

> „die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische

> Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke ... oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.“

Demgemäß muss zunächst die Erforderlichkeit (siehe Kapitel 6.10.3) der Daten nachgewiesen werden. Sodann muss das Gesetz nachweisen, dass die Zielsetzung des Gesetzes in Bezug auf die Einschränkung der Grundrechte der betroffenen Personen verhältnismäßig (siehe Kapitel 6.10) ist. Ist dies der Fall, so muss das Gesetz die Vorgaben der DS-GVO zum Schutz personenbezogener Daten berücksichtigen und „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorsehen. Diese Prüfung der bestehenden deutschen Gesetze ist zunächst erforderlich, bevor aufgrund dieser Gesetze Daten in Archive übermittelt werden dürfen, nachdem die DS-GVO gilt.

Diese Pflicht zur Überprüfung der entsprechenden Gesetze gilt natürlich analog bzgl. der Gesetze für die Gesundheitsstatistik.

7.3.7. Wissenschaftliche und historische Forschung

Siehe Kapitel 12.1

8. Betroffenenrechte

8.1. Übersicht

Kommentar:

Die heute existierenden Betroffenenrechte (= Recht auf Auskunft, Benachrichtigung, Berichtigung, Sperrung/Löschung, Widerruf) bleiben bestehen. Jedoch wurden die Rechte teilweise erweitert, z. B. muss beim Recht auf Auskunft künftig die Speicherdauer angegeben werden. Weiterhin kommen neue Rechte hinzu: das Recht auf Datenübertragbarkeit und das Recht, eine gemeinnützige Vereinigung mit der Wahrnehmung der eigenen Rechte gegenüber Gerichten und Behörden zu beauftragen.

Informationen gemäß den Artt. 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Artt. 15 bis 22 und Artikel 34 müssen entsprechend Art. 12 Abs. 5 unentgeltlich zur Verfügung gestellt werden, außer bei „offenkundig unbegründeten oder ... exzessiven Anträgen einer betroffenen Person“.

Grundsätzlich gilt: Hat der Verantwortliche begründete Zweifel an der Identität der Person, die ihre Rechte entsprechend Artt. 15 bis 21 wahrnimmt, so kann er die zusätzlichen Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind (Art. 12 Abs. 6 DS-GVO).

8.2. Information des Betroffenen

Die Rechte des Betroffenen bzgl. Auskunft / Information beruhen überwiegend auf den Artt. 13, 14.

8.2.1. Umfang der Informationspflicht

Kommentar:

Die Mindestinhalte, über die der Betroffene informiert werden muss, sind in Artt. 13, 14 DS-GVO angegeben. Hierzu zählen zum Zeitpunkt der Erhebung insbesondere die folgenden Informationen:

- Der Name und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters als auch des Datenschutzbeauftragten (sofern vorhanden)
- Die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen
- Die Rechtsgrundlage, auf welcher die Datenverarbeitung erfolgen darf
- Die Speicherdauer der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- Die Empfänger (bzw. ggfs. die Kategorien von Empfängern) der personenbezogenen Daten
- Die Informationen,
    - ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist,
    - ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte
- Der Hinweis, dass die Betroffenenrechte ausgeübt werden können, d. h. das Bestehen eines Rechts
    - auf Auskunft über die betreffenden personenbezogenen Daten,
    - auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung,
    - auf einen Widerspruch gegen die Verarbeitung,
    - auf Datenübertragbarkeit,

    - auf die Beschwerde bei einer Aufsichtsbehörde.
- Falls die Datenverarbeitung auf Grundlage einer Einwilligung beruht: zwingend erforderlich ist dann der Hinweis auf das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird
- Falls die Datenverarbeitung eine automatisierte Entscheidungsfindung beinhaltet: aussagekräftige Informationen über die involvierte Logik der automatisierten Entscheidungsfindung sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person
- Sofern vorgesehen: die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, inklusive der Rechtsgrundlage, welche die Übermittlung legitimiert (z. B. basierend auf einem Angemessenheitsbeschluss der Kommission)

8.2.2. Zeitrahmen der Auskunftserteilung

Kommentar:

Neu ist, dass der Verantwortliche gemäß Art. 12 Abs. 3 dem Auskunftsanspruch eines Betroffenen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags nachkommt. Im begründeten Einzelfall (= hohe Komplexität, Vielzahl von zeitgleichen Anfragen z. B. nach einer „Datenpanne“) kann diese Frist um zwei Monate verlängert werden. Über die Fristverlängerung wie auch der Begründung, warum es zu dieser kommt, muss der Betroffene jedoch innerhalb von 4 Wochen nach Antragstellung informiert werden.

8.2.3. Keine Informationspflicht bei Datenerhebung

Kommentar:

Eine Informationspflicht im Rahmen der Datenerhebung besteht nicht, „wenn und soweit die betroffene Person bereits über die Informationen verfügt“ (Artt. 13 Abs. 4, 14 Abs. 5). Entsprechend Art. 5 Abs. 2 DS-GVO muss der Verantwortliche nachweisen können, aus welchen Gründen der Betroffene nicht informiert wurde. Insbesondere ist hierzu natürlich auch der Nachweis erforderlich, auf welchem Wege die betroffene Person die verpflichtend anzugebenden Informationen wie beispielsweise die Speicherdauer auf anderem Wege erhielt.

Weiterhin besteht keine Informationspflicht, wenn die Daten nicht direkt beim Betroffenen erhoben wurden und einer der nachstehenden Gründe zutrifft (Art. 14 Abs. 5 DS-GVO):

- die Erteilung dieser Informationen erweist sich als unmöglich
- die Erteilung dieser Informationen erfordert einen unverhältnismäßigen Aufwand
- die Erlangung oder Offenlegung der personenbezogenen Daten ist durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, geregelt
- die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

8.2.4. Informationspflicht bei Zweckänderung

Kommentar:

Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den Ursprünglichen („Zweckänderung“), so muss er die betroffene Person vor der Weiterverarbeitung über diesen anderen Zweck informieren. Hierbei sind alle anderen maßgeblichen Informationen gemäß Artt. 13,14 DS-GVO (siehe auch Kapitel 8.2.1) dem Betroffenen zur Verfügung zu stellen (Artt. 13 Abs. 3, 14 Abs. 4 DS-GVO).

8.2.5. Information durch Bildsymbole

Kommentar:

Grundsätzlich können die in Artt. 13, 14 DS-GVO geforderten Information auch in Form von „standardisierten“ Bildsymbolen erfolgen (Art. 12 Abs. 7 DS-GVO). Dies soll dazu dienen, „in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln“. Im Rahmen der Verhandlungen wurde hier in erster Linie an die Information innerhalb von Apps auf Smartphones u. ä. gedacht; bedingt durch den begrenzten Darstellungsraum kann ein längerer Text ggfs. nicht die benötigten Informationen in klarer und verständlicher Weise bereitstellen. Ist die Informationsvermittlung durch Bildsymbole dann leichter möglich, so bietet sich diese Alternative an. Werden die Bildsymbole in elektronischer Form dargestellt, so müssen die Symbole maschinenlesbar sein. Auch bei dieser Form der Information muss der Verantwortliche ggfs. nachweisen, dass die betroffene Person die Informationen wahrnehmen und verstehen konnte (Art. 5 Abs. 2 DS-GVO), ein Nachweis, dass die Symbole angezeigt wurden, reicht hier nicht aus, da hierdurch das Verständnis der Bildsymbole nicht nachgewiesen werden kann.

8.2.6. Information bei Datenschutzvorfällen

Kommentar:

Der für die Verarbeitung Verantwortliche muss bei Datenschutzverstößen (z. B. einem Datenleck) oder bei einem hohen Risiko bzgl. eines Verstoßes entsprechend den Vorgaben von Art. 34 DS-GVO den Betroffenen selbst informieren. (Siehe Kapitel 9.9).

8.3. Auskunft

Fundstelle in der DS-GVO:

- Art. 15 „Auskunftsrecht der betroffenen Person“

Kommentar:

Das Recht der Betroffenen, welches derzeit aus dem BDSG herrührt, wird teilweise erweitert. So haben Betroffene jetzt beispielsweise auch das Recht, die Dauer der Speicherung zu erfragen.

8.3.1. Umfang der Auskunftspflicht

Kommentar:

Jeder Betroffene hat das Recht nachzufragen, ob von einem Verantwortlichen seine personenbezogenen Daten verarbeitet werden. Ist dies der Fall, so hat die betroffene Person das Recht zu erfahren, welche Daten dies sind. Weiterhin muss der Verantwortliche dem Betroffenen die Rahmenbedingungen, unter denen die Verarbeitung stattfindet, mitteilen. Zu diesen Informationen gehören insbesondere

- die Verarbeitungszwecke
- die Kategorien personenbezogener Daten
- die Empfänger oder Kategorien von Empfängern (auch geplante)
- die Speicherdauer der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- alle verfügbaren Informationen über die Herkunft der Daten (nur, wenn die Daten nicht bei der betroffenen Person selbst erhoben wurden)
- das Bestehen der Betroffenenrechte
    - das Recht auf Berichtigung durch den Verantwortlichen
    - das Recht auf Löschung oder auf Einschränkung der Verarbeitung der personenbezogenen Daten durch den Verantwortlichen
    - das Recht auf Widerspruch gegen diese Verarbeitung
    - das Recht zur Beschwerde bei einer Aufsichtsbehörde
- wenn eine automatisierte Einzelentscheidung oder ein Profiling unter Nutzung der personenbezogenen Daten durchgeführt wurde
    - aussagekräftige Informationen über die zur Entscheidungsfindung eingesetzte Logik
    - alle benötigten Informationen, damit die betroffene Person die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für sich erkennt
- bei Übermittlung in ein Drittland oder an eine internationale Organisation muss die Person informiert werden, welche Garantien zum Schutz der Daten des Betroffenen existieren.

8.3.2. Anspruch auf Kopie der Daten

Kommentar:

Weiterhin muss der Verantwortliche gemäß Art. 15 Abs. 3 DS-GVO der betroffenen Person eine vollständige Kopie der personenbezogenen Daten zur Verfügung stellen, wobei die erste Kopie kostenlos erfolgen muss. Weitere Kopien, die auf Anforderung der betroffenen Person erstellt werden, dürfen die Verwaltungskosten in Rechnung gestellt werden. Bei elektronischer Stellung eines Antrags auf Auskunft müssen die Informationen in einem „gängigen“ elektronischen Format zur Verfügung gestellt werden, sofern die Person nichts anderes verlangt.

8.4. Widerspruchsrecht

Fundstelle in der DS-GVO:

- Art. 21 „Widerspruchsrecht“

Kommentar:

Der Betroffene hat entsprechend Art. 21 Abs. 1 DS-GVO das Recht, der Verarbeitung zu widersprechen, wenn diese auf Art. 6 Abs. 1 Lit. e oder f DS-GVO gestützt ist. D. h. der Betroffene kann insbesondere einer Verarbeitung seiner Daten zur Wahrung berechtigter Interessen der verantwortlichen Stelle widersprechen, ohne dass schutzwürdige Belange des Betroffenen überwiegen.

Dies gilt ausdrücklich auch für Datenverarbeitungen zu Zwecken des Direktmarketings, einschließlich der Profilbildung für diese Zwecke (Art. 21 Abs. 2 und Abs. 2a DS-GVO), was für das Gesundheitswesen eine geringere Rolle spielt.

Insbesondere kann eine betroffene Person auch gegen eine auf Art. 89 Abs. 1 DS-GVO beruhende Verarbeitung der sie betreffenden Daten zu „wissenschaftlichen oder historischen

Forschungszwecken oder zu statistischen Zwecken“ Widerspruch einlegen. Es sei denn, die Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich. In diesem Fall muss der Verantwortliche sowohl die Erforderlichkeit (siehe Kapitel 6.10.3) als auch das öffentliche Interesse (siehe Kapitel 6.8) nachweisen.

Auf das Widerspruchsrecht ist der Betroffene „deutlich und getrennt” von jeglicher anderer Information hinzuweisen, und zwar spätestens „zum Zeitpunkt der ersten Kommunikation mit ihr“ (Art. 21 Abs. 2b DS-GVO).

Kann der Verantwortliche

- „zwingende schutzwürdige Gründe“ für die Verarbeitung nachweisen, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder
- die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen,

so muss dem Widerspruch nicht nachgekommen werden (Art. 21 Abs. 1 S. 2 DS-GVO). Entsprechend den Informationspflichten der DS-GVO ist die betroffene Person in diesem Fall sowohl über die weitere Verarbeitung als auch über die Gründe, weswegen dem Widerspruch nicht nachgekommen wird, zu benachrichtigen.

8.5. Recht auf Berichtigung und Vervollständigung

Fundstelle in der DS-GVO:

- Art. 16 „Recht auf Berichtigung“

Kommentar:

Das Recht der betroffenen Person auf Berichtigung umfasst neben dem Recht auf unverzügliche Korrektur unrichtiger personenbezogener Daten durch den Verantwortlichen auch das Recht auf eine Vervollständigung unvollständiger personenbezogener Daten, einschließlich einer ergänzenden Erklärung. Damit geht das Recht über die bisher existierenden gesetzlichen Regelungen in Deutschland bzgl. der Berichtigung falscher Daten (z. B. §6 Abs. 1 BDSG) hinaus: ein „Recht auf Vervollständigung“ vorhandener Daten gab es bisher nicht.

Der Verantwortliche muss gemäß Art. 19 DS-GVO zudem allen Empfängern der Daten, die berichtigt wurden, die Berichtigung mitteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Falls die betroffene Person dies wünscht, so muss der Verantwortliche die betroffene Person hiervon unterrichten (Art. 19 DS-GVO).

Hinweis: eine Aktualisierung ist keine Berichtigung!

8.6. Recht auf Löschen („Vergessenwerden“)

Fundstelle in der DS-GVO:

- Art. 17 „Recht auf Löschung („Recht auf „Vergessenwerden“)“

Kommentar:

Betroffene haben jetzt das Recht, dass die Daten unter bestimmten Bedingungen gelöscht werden. Zu diesen Bedingungen gehören insbesondere (Art. 17 Abs. 1 DS-GVO):

- Unionsrecht oder das Recht eines Mitgliedstaates, dem der Verantwortliche unterliegt, erfordern eine Löschung der personenbezogenen Daten.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung zur Verarbeitung ihrer Daten und eine andere Rechtsgrundlage existiert nicht.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine in Art. 21 Abs.2 genannten Gründe vor, dem Widerspruch nicht nachzukommen.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft mittels Einwilligung eines Kindes (Art. 8 Abs. 1 DS-GVO) erhoben.

8.6.1. Nebenpflichten

Kommentar:

Ist der Verantwortliche zur Löschung verpflichtet und hat die zu löschenden Daten öffentlich zugänglich gemacht, so „trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen“, um andere für die Datenverarbeitung Verantwortliche („Dritte“) darüber zu informieren, dass die Löschung aller Links zu diesen personenbezogenen Daten als auch die Löschung aller Kopien oder Replikationen dieser personenbezogenen Daten zu erfolgen hat (Art. 17 Abs. 2, Art. 19 DS-GVO).

Falls die betroffene Person dies wünscht, so muss der Verantwortliche die betroffene Person hiervon unterrichten (Art. 19 DS-GVO).

8.6.2. Ausnahmeregeln

Kommentar:

Eine Ausnahme sowohl von der Löschpflicht als auch von den Nebenpflichten existiert nur, wenn die Verarbeitung der Daten erforderlich ist

a) zur Ausübung des Rechts auf freie Meinungsäußerung und Information
b) zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt
c) zur Erfüllung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde
d) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
e) für
   - im öffentlichen Interesse liegende Archivzwecke,
   - wissenschaftliche oder historische Forschungszwecke oder
   - statistische Zwecke

   gemäß Art. 89 Abs. 1 DS-GVO, sofern die Löschung der personenbezogenen Daten die „Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt“
f) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

8.7. Recht auf Einschränkung der Verarbeitung („Sperrung“)

Fundstelle in der DS-GVO:

- Art. 18 „Recht auf Einschränkung der Verarbeitung“

Kommentar:

Das Recht des Zugriffs auf die Daten eines Betroffenen muss auf Aufforderung der betroffenen Person seitens des Verantwortlichen eingeschränkt werden, sofern eine der folgenden Voraussetzungen gegeben ist (Art. 18 Abs. 1 DS-GVO):

- Die Verarbeitung erfolgt unrechtmäßig, aber die betroffene Person lehnt die Löschung der sie betreffenden personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der sie betreffenden personenbezogenen Daten.
- Der Verantwortliche benötigt die Daten für die Verarbeitungszwecke nicht länger, die betroffene Person benötigt diese jedoch noch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird; in diesem Fall ist für die Dauer, die dem Verantwortlichen die Überprüfung der Angelegenheit ermöglicht, der Zugriff auf die Daten derart einzuschränken, dass die Daten nur noch zur Überprüfung der Angelegenheit verwendet werden können.
- Die betroffene Person erhebt Widerspruch gegen die Datenverarbeitung gemäß Art. 21 Abs. 1 DS-GVO und der Verantwortliche überprüft, ob seine berechtigten Gründe an der Verarbeitung der Daten gegenüber denen der betroffenen Person überwiegen; für die Dauer dieser Überprüfung ist der Zugriff auf die Daten derart einzuschränken, dass die Daten nur zur Überprüfung der Angelegenheit genutzt werden können.

Erfolgte eine Einschränkung der Daten, so dürfen diese Daten nur noch (Art. 18 Abs. 2 DS-GVO)

a) mit Einwilligung der betroffenen Person oder
b) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder
c) zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder
d) aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

Bevor eine Einschränkung aufgehoben wird, muss der Verantwortliche die betroffene Person davon unterrichten (Art. 18 Abs. 3 DS-GVO).

D. h.: Patientendaten, deren Verarbeitung eingeschränkt wurde (= Zugriff auf Daten wurde gesperrt), dürfen z. B. noch zu Abrechnungszwecken (= Geltendmachung von Rechtsansprüchen) genutzt werden, aber vor Aufhebung einer Sperrung muss der Patient unterrichtet werden. Auch wenn gesperrte Patientendaten zu Forschungszwecken entsperrt und verarbeitet werden sollen, muss der Patient vor Entsperrung der Daten informiert werden.

Es wäre daher wünschenswert, wenn künftig medizinische Informationssysteme entsprechende Benachrichtigungsfunktionen aufweisen. Dies bedingt natürlich, dass zum jeweiligen Patienten entsprechende Kontaktmöglichkeiten (z. B. E-Mail) im System hinterlegt werden.

Der Verantwortliche muss gemäß Art. 19 DS-GVO zudem allen Empfängern der Daten, deren Verarbeitung eingeschränkt wurde, bzgl. der Einschränkung der Verarbeitung informieren, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Falls die betroffene Person dies wünscht, so muss der Verantwortliche die betroffene Person hiervon unterrichten (Art. 19 DS-GVO).

8.8. Recht auf Datenübertragbarkeit

Fundstelle in der DS-GVO:

- Art. 20 „Recht auf Datenübertragbarkeit“

Kommentar:

Neu ist die Einführung eines Rechts auf „Datenübertragbarkeit“. Der Betroffene hat zum einen das Recht, seine, bei einem Dienstanbieter gespeicherten Bestandsdaten, in einer maschinenlesbaren Form zu erhalten (Art. 20 Abs. 1 DS-GVO), um sie so auf einen anderen Dienstanbieter übertragen zu können. Betroffene haben weiterhin das Recht, Bestandsdaten (z. B. Profile) zwischen Diensteanbietern zu transferieren, d. h. einen direkten Datentransfer zwischen altem und neuem Diensteanbieter zu veranlassen, wobei die technische Umsetzung dieser gesetzlichen Regelung offen ist (Art. 20 Abs. 2 DS-GVO).

Das Recht auf Datenübertragbarkeit gilt für Daten, die aufgrund einer Einwilligung (Art.6 Abs. 1 Lit. a bzw. Art. 9 Abs. 2 Lit. a) oder zur Erfüllung eines Vertrages (Art. 6 Abs. 1 Lit. b) verarbeitet werden und deren Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Bei einer Dokumentation zu der Behandlung eines Patienten wäre zu klären, ob diese zur Erfüllung des Behandlungsvertrages erhoben werden (Art. 8 Abs. 2 Lit. h) oder ob die Verarbeitung auf Grundlage einer Einwilligung gemäß Art. 9 Abs. 2 Lit. a stattfindet. Das Recht auf Datenübertragbarkeit würde im ersteren Fall nicht greifen, im Letzteren schon.

8.9. Verbandsklagerecht

Fundstelle in der DS-GVO:

- Art. 80 „Vertretung von betroffenen Personen“

Kommentar:

Nach Art. 80 Abs. 1 DS-GVO kann der Betroffene eine gemeinnützige Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht mit der Wahrnehmung seiner Rechte gegenüber Gerichten und Behörden beauftragen. Dies gilt bzgl. Vertretung für

- Beschwerderecht bei einer Aufsichtsbehörde (Art. 77)
- Beschwerderecht auf gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde (Art. 78)
- Beschwerderecht auf wirksamen gerichtlichen Rechtsbehelf gegen für die Verarbeitung Verantwortliche oder Auftragsverarbeiter (Art. 79)
- Schadensersatzanspruch (Art. 82).

8.10. One-Stop-Shop

Kommentar:

Grundsätzlich soll ein betroffener Bürger (oder auch ein Unternehmen) in Europa einen „Ansprechpartner“ in Form der Aufsichtsbehörde haben, sodass der Bürger nicht herausfinden muss „welche Aufsichtsbehörde ist in diesem Fall zuständig?“. Vielmehr wendet er sich an eine Aufsichtsbehörde, die dann die Angelegenheit für ihn klärt: alle notwendigen bürokratischen Schritte, die zur Erreichung eines Zieles führen, werden für den betroffenen Bürger von einer einzigen Stelle durchgeführt.

Dabei gilt der Grundsatz der Zuständigkeit im eigenen Hoheitsgebiet entsprechend Art. 51 DS-GVO. Bei grenzüberschreitender Verarbeitung gibt es eine „federführende“ Aufsichtsbehörde. Gemäß Art

56 Abs. 1 DS-GVO ist die federführende Aufsichtsbehörde diejenige Aufsichtsbehörde, die für die Hauptniederlassung zuständig ist. Die federführende Aufsichtsbehörde arbeitet laut Art. 56 Abs. 3 DS-GVO bzw. Art 56. Abs. 4 DS-GVO i. V. m. Art. 60 DS-GVO mit der oder den betroffenen Aufsichtsbehörden (siehe Begriffsbestimmung in Art. 4 Abs. 22 DS-GVO) zusammen.

9. Datenverarbeitung im Unternehmen

Kommentar:

Die Artikel 24-43 DS-GVO enthalten die verschiedensten Pflichten für Unternehmen, die personenbezogene Daten für eigene Zwecke sammeln und verarbeiten bzw. nutzen, insbesondere auch im Bereich der Auftragsdatenverarbeitung.

9.1. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Fundstelle in der DS-GVO:

- Art. 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“

Kommentar:

„Data protection by design and by default”, Begriffe, die bereits seit langem diskutiert wurden, sind nunmehr in der DS-GVO explizit geregelt.

Um das Prinzip von „Privacy by Design“ bzw. „data protection by design“ nachvollziehen zu können, ist es zunächst essenziell zu klären, wer eigentlich bei der VO zu „data protection by design“ verpflichtet wird. Ginge man zunächst nur von dem Begriff aus, würde man schnell den Herstellern die Verantwortung für „data protection by design“ in ihren Produkten zuweisen. Doch eine solche Zuweisung würde der Systematik des Datenschutzrechts zuwider laufen, wonach primär der Verantwortliche und sekundär der Auftragsverarbeiter Verpflichteter ist. Und dieser Problematik zollt auch Art. 25 Abs. 1 entsprechend Tribut. So heißt es: „*Unter Berücksichtigung des Stands der Technik und der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die persönlichen Rechte und Freiheiten trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, mit denen die wirksame Umsetzung der Datenschutzgrundsätze wie etwa Datenminimierung und die Aufnahme der notwendigen Garantien in die Verarbeitung erreicht werden sollen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.*“

Letztendlich sagt Art. 25 Abs. 1 deshalb ganz klar, dass der Verantwortliche derjenige ist, der „data protection by design“ in seiner Organisation implementieren muss. Daher muss er konsequentermaßen seine Unternehmensprozesse analysieren und die entsprechenden erforderlichen technischen und organisatorischen Maßnahmen (by Design) in seine Prozesse implementieren (Risikomanagement). Und dabei gilt es immer, auch die Kosten und den Nutzen zu beachten.

Die DS-GVO adressiert auch den Hersteller von Produkten. Jedoch nicht so, wie man es erwarten würde. Denn die Pflicht des Herstellers zu „datenschutzfreundlicher Technik“ kann nicht von ihm abverlangt werden. So heißt es in ErwGr. 78: „*In Bezug auf Entwicklung, Auslegung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen*

zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. "

Damit wird abermals klargestellt, dass Verpflichteter bei „data protection by design" der Verantwortliche ist und bleibt. Hersteller können nur zu „data protection by design" verpflichtet sein, wenn sie selber als Verantwortlicher angesehen werden können.

Dieses hat zur Konsequenz, dass gerade bei zu beschaffenden Neusystemen der Verantwortliche verpflichtet ist, gem. Art. 35 eine DatenschutzFolgenabschätzung (Vorabkontrolle) durchzuführen und dabei insbesondere zu prüfen, ob sich mit diesem System „data protection by design" entsprechend gewährleisten lässt.

Es empfiehlt sich deshalb, bei Neuanschaffungen „data protection by design" in (öffentlichen) Ausschreibungen sowie den entsprechenden Anforderungsprofilen unbedingt zu berücksichtigen (ErwGr. 78).

Durch die gesetzliche Pflicht des Verantwortlichen zum Einsatz „datenfreundlicher Technik" wird letztlich ein mittelbarer Druck auf die Hersteller entstehen. Dieses insbesondere deshalb, weil durch die Regelungen der DS-GVO, der Verantwortliche keine (Neu-) Produkte ohne bzw. mit unzureichender „data protection by design" kaufen bzw. einsetzen darf. Neusysteme, die kein „data protection by design" implementiert haben, dürften deshalb (nach Intention des Gesetzgebers) nicht mehr nachgefragt werden, sodass sich die Umsetzung dieser Anforderungen durch die „Macht des Marktes" von alleine regeln wird.

Für Altsysteme ergibt sich prinzipiell auch nichts Neues. Bei enger Auslegung der Regelungen der DS-GVO lässt sich daraus ableiten, dass man als Verantwortlicher seine Alt-Systeme danach überprüfen muss, ob mit diesen die Anforderungen nach „data protection by design" erfüllt werden können. Für „kritische" Alt-Produkte, mit denen bspw. Gesundheitsdaten verarbeitet werden (Medizinprodukte / KIS), empfiehlt sich deshalb eine gründliche Prüfung vorzunehmen (heute im Rahmen einer verstärkten „Vorabkontrolle"), wobei man jedoch auch immer die „Wirtschaftlichkeit" beachten sollte. Trifft man bei dieser Überprüfung auf (eklatante) „Mängel", sollte man diese offen mit den Herstellern diskutieren und gemeinsam Lösungen entwickeln.

Darüber hinaus sollten nach der DS-GVO ferner in allen Systemen „data protection by default" enthalten bzw. umsetzbar sein. Dieser Grundsatz findet sich in Art. 25 Abs. 2 wieder in dem es heißt: „*Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden; dies gilt für den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht ohne Eingreifen einer natürlichen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden*."

Ein Verantwortlicher sollte deshalb überprüfen, ob die von ihm eingesetzte Soft- und Hardware „datenschutzfreundliche Voreinstellungen" enthält, bzw. ob man solche Einstellungen nachträglich noch vornehmen kann.

Der Gedanke, dem „data protection by default" zugrunde liegt, ist durchaus nachvollziehbar. Anwender sollten sich durch etwaige Voreinstellungen weniger Gedanken um die Einhaltung des Datenschutzes bei der Anwendung machen müssen.

9.1.1. Literatur

- European Union Agency for Network and Information Security (ENISA) (2015) Privacy and Data Protection by Design. Online, zitiert am 2016-05-12; Verfügbar unter https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
- European Union Agency for Network and Information Security (ENISA) (2016) Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. Online, zitiert am 2016-05-12; Verfügbar unter https://www.enisa.europa.eu/publications/pets
- Forum Privatheit (2016) White Paper Datenschutz-Folgenabschätzung - Ein Werkzeug für einen besseren Datenschutz. Online, zitiert am 2016-04-21; Verfügbar unter https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum_Privatheit_White_Paper_Datenschutz-Folgenabschaetzung_2016.pdf
- Microsoft (2012) Differential Privacy for Everyone. Online, zitiert am 2016-05-12; Verfügbar unter http://www.microsoft.com/en-us/download/details.aspx?id=35409

9.2. Gemeinsam für die Verarbeitung Verantwortliche

Fundstelle in der DS-GVO:

- Art. 26 „Gemeinsam für die Verarbeitung Verantwortliche“

Kommentar:

Neu für Deutschland ist die Möglichkeit, dass zwei oder mehrere Verantwortliche gemeinsam die Zwecke und Mittel festlegen können. Da diese Vorgabe der RL 95/46/EG nie in deutsches Recht umgesetzt wurde, kommen deutsche Unternehmen erst durch die direkte Wirkung der DS-GVO mit dieser Regelung in Berührung. Hierbei müssen transparente Regelungen zur Verantwortlichkeit für die Einhaltung der Datenschutzregelungen getroffen werden, denn dem Betroffenen muss transparent dargelegt werden, welcher Verantwortliche bzgl. welcher Mittel/Zwecke Ansprechpartner ist. Die Rechte des Betroffenen dürfen dadurch, dass nicht ein, sondern mehrere Verantwortliche existieren, nicht gemindert werden. Insbesondere kann die betroffene Person ihre Rechte (Artt. 12 – 22) grds. bei jedem der Verantwortlichen geltend machen.

Nach dieser für Deutschland „neuen“ Rechtsfigur der DS-GVO ist es explizit möglich, dass sich zwei oder mehr Verantwortliche für die Datenverarbeitung verantwortlich zeichnen und gemeinsamen über die Mittel und Zwecke der Datenverarbeitung entscheiden (siehe auch ErwGr. 79).

Die gemeinsam für die Verarbeitung Verantwortlichen haben mit dem Begriff des „Auftragsverarbeiter“ jedoch nichts zu tun: der Auftragsverarbeiter handelt nur auf Weisung und darf somit nicht über Mittel und Zwecke der Datenverarbeitung entscheiden.

9.3. Sicherheit der Verarbeitung

Fundstelle in der DS-GVO:

- Art. 32 „Sicherheit der Verarbeitung“

Kommentar:

Die Verantwortlichen treffen geeignete Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Gesundheitsdaten als besondere Kategorie von Daten erfordern auf jeden Fall ein hohes Schutzniveau. In die Abwägung bzgl. der zu treffenden technischen und organisatorischen Maßnahmen zur Herstellung eines dem Risiko angemessenen Schutzniveaus sind insbesondere zu berücksichtigen (Art. 32 Abs. 1 DS-GVO):

- Der Stand der Technik[28]
- Die Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Diese Maßnahmen schließen u.a. Folgendes ein (Art. 32 Abs. 1 DS-GVO):

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die Anforderungen der DS-GVO stehen damit im Einklang mit den Ausführungen des Bundesverfassungsgerichts im Urteil bzgl. der (heimlichen) Online-Durchsuchung (Urteil bzgl. „Grundrecht auf Vertraulichkeit und Integrität von IT-Systemen“)[16].

Die Mitgliedstaaten und die Aufsichtsbehörden fördern die Ausarbeitung von Verhaltensregeln, Zertifikaten und Datenschutzprüfsiegeln (Artt. 40 bis 43). Diese Mittel sollen es dem Verantwortlichen erleichtern, die Anforderungen bezüglich der Sicherheit der Verarbeitung zu erfüllen. (Kein Katalog / Checkliste mehr wie z. B. nach Anlage zu § 9 BDSG, vielmehr Schutzprinzipien)

9.4. Konzernprivileg

Fundstelle in der DS-GVO:

- Art. 47 „Verbindliche interne Datenschutzvorschriften“

Kommentar:

Ein echtes Konzernprivileg gibt es auch in der DS-GVO nicht. Es gibt jedoch einige Regelungen die eine Konzentrierung erleichtern.

Ein Unternehmen kann europaweit tätig sein und mit Haupt- und Nebenneiderlassungen lokal präsent sein. Ebenfalls ist die gemeinsame Datenverarbeitung erlaubt, wenn es eine Unternehmensgruppe ist, in der ein Unternehmen verbindlich Vorschriften durchsetzen kann.

Auch die Übermittlung der Daten in ein Drittland kann innerhalb einer Gruppe von Unternehmen durch verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) möglich sein, wenn die Aufsichtsbehörde diese genehmigt.

Damit können z. B. Beschäftigtendaten zugunsten einer zentralen Personalverwaltung innerhalb einer Unternehmensgruppe übermittelt werden.

[16] Bundesverfassungsgericht Urt. v. 27.02.2008, Az.: 1 BvR 370/07 und 1 BvR 595/07. Online, zitiert am 2016-05-19; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Text=1%20BvR%20370/07 bzw. http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html

9.5. Datenschutz-Folgenabschätzung (Vorabkontrolle)

Fundstelle in der DS-GVO:

- Art. 35 „Datenschutz-Folgenabschätzung“
- Art. 36 „Vorherige Konsultation“

Kommentar:

Für Verarbeitungen, „die aufgrund ihres Wesens, ihres Umfangs oder ihrer Zwecke konkrete Risiken für die Rechte und Freiheiten betroffener Personen bergen“, müssen Unternehmen die Folgen abschätzen und ihre Maßnahmen dokumentieren. Im Prinzip ist die Datenschutz-Folgenabschätzung aus der Vorabkontrolle des BDSG bekannt, jedoch steigen die Anforderungen an die formale Dokumentation und die Aufsichtsbehörde kann diese Unterlagen anfordern. Eine Datenschutz-Folgenabschätzung muss gemäß Art. 35 Abs. 7 DS-GVO zumindest die nachfolgend genannten Punkte beinhalten:

- eine systematische Beschreibung
  - der geplanten Verarbeitungsvorgänge
  - der Zwecke der Verarbeitung
  - Ggfs. die vom Verantwortlichen verfolgten berechtigten Interessen
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck (siehe auch Kapitel 6.10)
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen (siehe auch Kapitel 6.10)
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren,
  - durch die der Schutz personenbezogener Daten sichergestellt und
  - der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird,
  - wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Grundsätzlich wird eine Datenschutz-Folgenabschätzung erforderlich ein, wenn Daten der besonderen Art wie z. B. Gesundheitsdaten verarbeitet werden, da eine Verarbeitung dieser Daten per definitionem ein hohes Risiko für den Betroffenen beinhaltet. Auch Verarbeitungen, welche „neue“ Techniken wie beispielsweise RFID und Big Data zur Verarbeitung nutzen, also die Art der Verarbeitung ändern, bergen entsprechende Risiken und werden vermutlich eine Datenschutz-Folgenabschätzung erforderlich machen. Auch für die Videoüberwachung z. B. wird eine Datenschutz-Folgenabschätzung für notwendig erachtet.

Durch die Aufsichtsbehörden sind noch Listen von Verfahren zu erstellen, bei denen sie nie bzw. immer eine Folgenabschätzung erwarten.

Bei Verfahren, die ein hohes Risiko zur Folge haben, sollte der Verantwortliche immer die Aufsichtsbehörde konsultieren. Im Gegensatz zum BDSG muss die Aufsichtsbehörde die Konsultation innerhalb 8 bzw. 14 Wochen beantworten.

Die Befreiung für Unternehmen mit weniger als 250 Mitarbeitern gilt bei der Verarbeitung von Gesundheitsdaten nicht.

9.6. Verzeichnis von Verarbeitungstätigkeiten (Verfahrensverzeichnis)

Fundstelle in der DS-GVO:

- Art. 30 „Verzeichnis von Verarbeitungstätigkeiten“

Kommentar:

Art. 30 enthält eine Dokumentationspflicht, die auch für Auftragsverarbeiter gilt, und diese wird das heutige Verfahrensverzeichnis ersetzen. Diese Dokumentation ist, wie das Verfahrensverzeichnis heute auch, für die Aufsichtsbehörden bereitzuhalten. Die Dokumentation soll die wesentlichen Informationen zusammenfassen wie Angaben zur verantwortlichen Stelle, den verwendeten Daten bzw. Datenarten, dem Zweck der Verarbeitung, Löschfristen und Empfänger sowie eine Darstellung der getroffenen organisatorischen und technischen Maßnahmen zur Gewährleistung der Sicherheit der Daten. D. h. die Inhalte der vorgeschriebenen Dokumentation entsprechen weitestgehend den Inhalten des heutigen Verfahrensverzeichnisses.

Eine vergleichende Übersicht der Anforderungen von Art. 30 Abs. 1 DS-GVO und §4e BDSG bzgl. der Verfahrensdokumentation gibt die nachfolgende Tabelle:

Art. 30 Abs. 1 DS-GVO	§4e BDSG
a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;	1. Name oder Firma der verantwortlichen Stelle 2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen, 3. Anschrift der verantwortlichen Stelle,
b) die Zwecke der Verarbeitung	4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung
c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;	5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien
d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;	6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;	8. eine geplante Datenübermittlung in Drittstaaten
f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;	7. Regelfristen für die Löschung der Daten

Art. 30 Abs. 1 DS-GVO	§4e BDSG
g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.	9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind

Tabelle 1: Verzeichnis von Verarbeitungstätigkeiten vs. Verfahrensverzeichnis

Es gilt jedoch zu beachten, dass wir nicht mehr das „Jedermann-Verzeichnis“ haben. Die Betroffenen können jetzt auch nicht mehr Einsicht in dieses verlangen, sondern haben vielmehr ihre Auskunftsrechte.

9.7. Datenübermittlung (in Drittstaaten)

Kommentar:

Das europäische Rechtssystem wurde geschaffen, um den Handel im europäischen Binnenmarkt zu erleichtern. Darauf weist auch Art. 1 Abs. 3 hin: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden“. Desgleichen Erwägungsgrund 10: „Um ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein“.

Demgemäß muss insbesondere die Übermittlung personenbezogener Daten an Drittländer oder international tätige Organisationen aus Sicht der DS-GVO geregelt werden, denn innerhalb von Europa existiert ja überall ein adäquates Datenschutzrecht. Die Artt. 44 bis 50 in Kapitel V sind damit auch dieser Situation gewidmet.

9.7.1. Allgemeine Grundsätze

Fundstelle in der DS-GVO:

- Art. 44 „Allgemeine Grundsätze der Datenübermittlung“

Kommentar:

Wie bisher ist eine Verarbeitung in einem Drittland erlaubt, wenn dort ein angemessenes Schutzniveau vorhanden ist. Entsprechend Art. 44 DS-GVO ist für die Einhaltung der Vorgaben neben dem Verantwortlichen ggfs. auch der Auftragsverarbeiter verantwortlich. D. h. wenn ein Verstoß durch den Auftraggeber verursacht wurde, dann wird ggfs. auch dieser mit einem Bußgeld bestraft, welches bis zu 20 000 000 Euro oder im Fall eines Unternehmens bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen kann.

Dies gilt gemäß Art. 44 DS-GVO auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. D. h., wenn aufgrund der in einem Drittland geltenden Regelungen personenbezogene Daten unrechtmäßig im Sinne der DS-GVO weitergegeben werden, sind dafür der Verantwortliche und ggfs. auch der Auftragsverarbeiter verantwortlich.

9.7.2. Angemessenheitsbeschluss

Fundstelle in der DS-GVO:

- Art. 45 „Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses“

Kommentar:

Art 45 räumt der Europäischen Kommission das Recht ein, Länder, Gebiete oder Sektoren in einem Drittland zu benennen, die ein angemessenes Schutzniveau haben. Die Kommission kann somit ein angemessenes Datenschutzniveau auch für ein Gebiet oder ein oder mehrere spezifische Sektoren eines Drittlands feststellen. Somit kann ggfs. die Übermittlung in einen Teilbereich statthaft sein, auch wenn das Drittland als Ganzes als „unsicher“ eingestuft bleibt.

9.7.3. Standarddatenschutzklauseln

Fundstelle in der DS-GVO:

- Art. 46 „Datenübermittlung vorbehaltlich geeigneter Garantien

Kommentar:

Sollte für das Land kein (pauschaler) Angemessenheitsbeschluss vorliegen, können über einen Vertrag nach den Standarddatenschutzklauseln oder verbindliche interne Datenschutzvorschriften die für die Übermittlung notwendigen Garantien gegeben werden.

Die derzeit geltenden Standardvertragsklauseln [17] behalten entsprechend ErwGr. 171 ihre Gültigkeit, bis sie entweder von der Kommission oder dem EuGH für ungültig erklärt werden. Hierbei muss beachtet werden, dass in den aktuellen Standardvertragsklauseln in Klausel 5 die Pflichten des Datenimporteurs (also die Stelle im Drittland) beschrieben werden. Bei Anwendung der vorliegenden Standardvertragsklausen garantiert der Datenimporteur, dass

- er die personenbezogenen Daten nur im Auftrag des Datenexporteurs und in Übereinstimmung mit dessen Anweisungen und den vorliegenden Klauseln verarbeitet; dass er sich, falls er dies aus irgendwelchen Gründen nicht einhalten kann, bereit erklärt, den Datenexporteur unverzüglich davon in Kenntnis zu setzen,
- er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen.

D. h. die rechtlichen Rahmenbedingungen im Drittland müssen dergestalt sein, dass der Datenimporteur diesen Vertragsanforderungen genügen kann.

Die Pflichten des Datenexporteurs (dies ist der Verantwortliche entsprechend DS-GVO) werden in Klausel 4 beschrieben. U.a. muss der Verantwortliche „die betroffene Person bei der Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung davon in Kenntnis“ setzen, dass „ihre Daten in ein Drittland übermittelt werden könnten, das kein angemessenes Schutzniveau“ aufweist. D. h. letztlich, dass ggfs. jeder Patient von der Möglichkeit informiert werden muss, dass seine Daten (z. B. im Rahmen einer Fernwartung oder einer entsprechenden Support-Dienstleistung) in einem Drittland verarbeitet werden.

[17] EU-Kommission: Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern. [Online, zitiert am 2016-05-26]; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1445851652852&uri=CELEX:32010D0087

9.7.4. Interne Datenschutzvorschriften / BCR

Fundstelle in der DS-GVO:

- Art. 47 „Verbindliche interne Datenschutzvorschriften“

Kommentar:

Das bisher bekannte Instrument „Binding Corporate Rules“ wurde in die Regulation aufgenommen. Wie bisher muss die Aufsichtsbehörde diesen Vertrag genehmigen.

Binding Corporate Rules (BCR) sind ein Konstrukt für verbindliche Richtlinien zum Umgang mit den eigenen personenbezogenen Daten innerhalb der eigenen Konzernstruktur[18,19]. Basierend auf diesen Richtlinien dürfen internationale Institutionen, Organisationen und Firmen nach geltendem europäischem Recht, personenbezogene Daten in Drittstaaten mit nicht angemessenem Datenschutzniveau transferieren, sofern die BCR von der zuständigen Aufsichtsbehörde genehmigt wurden.

Um den Umgang mit BCR zu erleichtern, veröffentlichte die Artikel-29-Datenschutzgruppe verschiedene Leitlinien, z. B.

- Working Paper 212 (2014-02): Anforderungen an verbindliche unternehmensinterne Regelungen, die den nationalen Datenschutzbehörden der EU vorgelegt werden, und an Regelungen für den grenzüberschreitenden Datenschutz, die den von der APEC anerkannten „CBPR Accountability Agents“ vorgelegt werden (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_de.pdf)
- Working Paper 204 (2013-04): Erläuterndes Dokument zu verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsverarbeiter (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_de.pdf)
- Working Paper 195 (2012-06): Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_de.pdf)
- Working Paper 155 (2008-06): FAQ zu Binding Corporate Rules (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp155_rev.04_de.pdf)
- Working Paper 154 (2008-06): Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_de.pdf)
- Working Paper 153 (2008-06): Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_de.pdf)
- Working Paper 133 (2007-01): Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc)

[18] EU-Kommission: Letters and other documents. [Online, zitiert am 2016-05-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm

[19] EU-Kommission: Binding Corporate rules. [Online, zitiert am 2016-05-26]; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/bcr/index_en.htm

- Working Paper 108 (2005-04): Muster-Checkliste für Anträge auf Genehmigungen verbindlicher unternehmensinterner Datenschutzregelungen (BCR) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_de.pdf)
- Working Paper 107 (2005-04): „Festlegung eines Kooperationsverfahrens zwecks Abgabe gemeinsamer Stellungnahmen zur Angemessenheit der verbindlich festgelegten unternehmensinternen Datenschutzgarantien (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_de.pdf)
- Working Paper 102 (2004-11): Muster-Checkliste „Antrag auf Genehmigung verbindlicher Unternehmensregelungen (BCR)“ (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp102_de.pdf)
- Working Paper 74 (2003-06): Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_de.pdf)

9.7.5. Unzulässige Übermittlung / unzulässige Offenlegung

Fundstelle in der DS-GVO:

- Art. 48 „Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung“

Kommentar:

Kommentar:

Entsprechend Art. 48 DS-GVO sind Gesetze von Drittländern, Entscheidungen von Behörden oder auch in einem Drittland gefällte Gerichtsurteile, welche von einem Verantwortlichen die Übermittlung oder Offenlegung personenbezogener Daten fordern, nur dann statthaft, wenn die Aufforderung aus dem Drittland auf eine in Kraft befindliche internationale Übereinkunft (z. B. ein Rechtshilfeabkommen) zwischen dem Drittland und der Union oder bzw. dem Mitgliedsstaat, in welchem der Verantwortliche tätig ist und dessen Rechtsprechung er unterliegt, gestützt ist.

Ohne entsprechende Übereinkunft ist eine Übermittlung oder Offenbarung personenbezogener Daten nicht statthaft und entspricht einem Bußgeldtatbestand gemäß Art. 83 Abs. 5 Lit. c DS-GVO, der mit einem Bußgeld bis zu 20 000 000 Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet wird.

9.7.6. Ausnahmeregelungen

Fundstelle in der DS-GVO:

- Art. 49 „Ausnahmen für bestimmte Fälle“

Kommentar:

Gemäß Art 49 Abs. 1 Lit. a DSGVO ist es möglich, personenbezogene Daten auf Basis einer Einwilligung oder zur Erfüllung eines Vertrages zu übermitteln, auch wenn für das jeweilige Drittland das Vorliegen eines Angemessenheitsbeschlusses der Kommission nicht gegeben ist und das Drittland auch keine geeigneten Garantien für die Sicherheit der personenbezogenen Daten aufweist.

Entsprechend Art. 49 Abs. 1 Lit. b DS-GVO ist die Übermittlung statthaft, wenn sie für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist.

Weiterhin ist die Übermittlung personenbezogener Daten eines Betroffenen in ein Drittland statthaft, wenn dies zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich ist. Im Sinne der Behandlung eines Betroffenen durch einen Arzt kann somit die Übermittlung medizinischer Daten in ein Drittland im Rahmen eines Behandlungsvertrages statthaft sein, wenn beispielsweise die bestmögliche medizinische Versorgung nur durch die Verarbeitung in einem Drittland gewährleistet werden kann und Alternativen nicht gegeben sind.

9.8. Auftragsdatenverarbeitung

Kommentar:

Überwiegend entsprechen die Begriffsbestimmungen bzgl. Auftragsverarbeitung der DS-GVO denen der Richtlinie 95/46/EG. Bei der Umsetzung der RL 95/46/EG orientierte sich der Gesetzgeber bzgl. dieser Begrifflichkeiten an dem Text des BDSG 1990, nicht am Text der Richtlinie. Daraus resultiert, dass sich in Deutschland durch die DS-GVO das Verständnis bzgl. Auftragsverarbeitung ändern muss. Zur Interpretation der Begrifflichkeiten sollten daher die bisherigen Ausführungen der Artikel-29-Datenschutzgruppe zur Interpretation der Begrifflichkeiten der RL 95/46/EG herangezogen werden[20].

Die DS-GVO weist nicht eine so starke technische Ausprägung bzgl. Auftragsverarbeitung auf wie das BDSG, sondern ist stärker funktional geprägt. D. h. es steht nicht immer nur die technische Ausprägung eines Auftrags im Vordergrund, wie es beispielsweise bei der Wartung von IT-Systemen der Fall ist, sondern Auftragsverarbeitung kann beispielsweise auch die Auslagerung von Postdienstleistungen (siehe Beispiel 17 in Fußnote 4) umfassen. In der Richtlinie war – ebenso wie jetzt in der DS-GVO – auch vorgesehen, dass es mehr als einen Verantwortlichen geben kann (siehe Kapitel 9.2). Weiterhin kann entsprechend RL als auch nach der DS-GVO der Auftragsverarbeiter eigenverantwortliche Spielräume für die Umsetzung des Auftrags eingeräumt bekommen; entscheidend ist, dass der Auftraggeber als Verantwortlicher einen rechtlichen (ggfs. auch einen tatsächlichen) Einfluss auf die Entscheidung bzgl. der Verarbeitung der Daten hat.

9.8.1. Auswahl Auftragsverarbeiter, Unterauftragnehmer und ADV-Vertrag

Fundstelle in der DS-GVO:

- Artikel 28 „Auftragsverarbeiter“

Kommentar:

Wie bisher muss der (bzw. müssen die) Verantwortliche(n) als Auftraggeber den Auftragnehmer sorgfältig auswählen. Der Auftragnehmer darf nur beauftragt werden, wenn dieser ausreichend Garantien bietet, dass den Vorgaben der DS-GVO bzgl. der Sicherheit der Datenverarbeitung genügt wird (Art. 28 Abs. 1 DS-GVO).

Unterauftragnehmer müssen durch den Verantwortlichen genehmigt werden. Existiert eine „allgemeine schriftliche Genehmigung“ bzgl. Hinzuziehung von Unterauftragnehmern, so muss der Auftragnehmer den Verantwortlichen vor Beauftragung eines Unterauftragnehmers oder Änderung einer Unterauftragnehmerschaft informieren, sodass dieser Einspruch erheben kann (Art. 28 Abs. 2 DS-GVO).

[20]Working Paper 169 (2010-02): „Für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“. Online, zitiert am 2016-05-19; Verfügbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

Werden Datenverarbeitungsvorgänge ausgelagert, so müssen die Details in einem begleitenden Auftragsdatenverarbeitungsvertrag festgehalten werden (Art. 28 Abs. 3 DS-GVO). Die Anforderungen sind denen von §11 BDSG ähnlich, jedoch nicht völlig identisch. Insbesondere müssen bestehende ADV-Verträge auch hinsichtlich

- der Umsetzung der sicherheitstechnischen Anforderungen der DS-GVO
- der Bestimmungen bzgl. Unterauftragsverhältnissen
- den Informationspflichten
    - Hinweispflicht seitens Auftraggebers bei rechtswidrigen Weisungen durch den Auftraggeber/Verantwortlichen
    - Hinweispflicht des Auftraggebers bzgl. Übermittlung in ein Drittland
- den Dokumentationspflichten des Auftragnehmers
    - Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten
    - Dokumentationspflicht hinsichtlich der Weisungen
- den Unterstützungspflichten des Auftragnehmers
    - Dokumentation bzgl. des Verzeichnisses von Verarbeitungstätigkeiten durch den Auftraggeber/Verantwortlichen
    - Bei der Zusammenarbeit mit den Aufsichtsbehörden
    - Bei der Meldung von Datenpannen
- des Umgangs mit der Datenverarbeitung in einem Drittland insbesondere der diesbezüglichen Weisungsabhängigkeit des Auftragnehmers

bzgl. ihrer Verordnungskonformität geprüft werden. Viele der Punkte, die nicht explizit in §11 BDSG vorhanden waren, sind in den meisten Vertragsmustern bereits enthalten, sodass sich der Anpassungsbedarf vermutlich in Grenzen hält.

Allerdings muss auch die Form des ADV-Vertrages selbst überprüft werden. §11 BDSG sprach nur von einem Auftrag, die Formvorschrift eines Vertrages mit den entsprechenden aus dem BGB resultierenden Anforderungen an einen Vertrag fand sich so nicht in den datenschutzrechtlichen Folgen. Vielmehr erfüllte jedes Dokument, welches den inhaltlichen Anforderungen genügte, als ausreichend. Art, 28 Abs. 3 DS-GVO verlangt nun ausdrücklich einen Vertrag oder „ein anderes Rechtsinstrument“. Gemäß Art. 28 Abs. 9 DS-GVO muss der Vertrag schriftlich abgefasst werden, wobei eine entsprechende Schriftform auch ein elektronisches Format aufweisen darf.

9.8.2. Dokumentationspflichten des Auftragnehmers

Fundstelle in der DS-GVO:

- Artikel 30 „Verzeichnis von Verarbeitungstätigkeiten“

Kommentar:

Zentrale Verfahren müssen schriftlich dokumentiert werden, wobei die schriftliche Dokumentation in einem elektronischem Format erfolgen kann. Die Angaben, die der Auftragsverarbeiter angeben muss, entsprechen weitestgehend denen des Auftraggebers:

- Den Namen und die Kontaktdaten des oder der Auftragsverarbeiters
- Den Namen und die Kontaktdaten des oder der Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist
- Den Namen und die Kontaktdaten aller etwaigen Vertreter der für die Verarbeitung Verantwortlichen
- Wenn vorhanden: Namen und die Kontaktdaten des Datenschutzbeauftragten

- Die Kategorien von Datenverarbeitungen
- Wenn zutreffend: Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie die Dokumentierung geeigneter Garantien
- Eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

9.8.3. Haftungsfragen

Fundstelle in der DS-GVO:

- Art. 82 „Haftung und Recht auf Schadenersatz“

Kommentar:

Auftraggeber und Aufragnehmer stehen nun gemeinsam gegenüber der betroffenen Person für einen Datenschutzverstoß ein. D. h. für den Auftraggeber ändert sich bzgl. der Haftung gegenüber dem Betroffenen nichts. Für den Auftragnehmer erhöht sich jedoch das Risiko im Vergleich zu heute: Geschädigte können Ansprüche auch ihm gegenüber geltend machen.

Eine Partei kann sich jedoch exkulpieren.

9.9. Meldepflichten

Fundstelle in der DS-GVO:

- Artikel 33 „Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde“.
- Art. 34 „Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person“.

Kommentar:

Im Fall von bestimmten Datenverlustszenarien müssen die Betroffenen sowie die Datenschutz-Aufsichtsbehörden informiert werden.

Meldepflichten sind ein wesentliches Element, um entsprechende Transparenz und die Betroffenenrechte bei einer „Datenpanne“ zu wahren. Ferner sollen diese Meldungen den Betroffenen ermöglichen, dass sie für die durch die Datenpanne nun drohenden Risiken entsprechende Maßnahmen treffen (können), um sich bspw. so gut wie möglich vor einem Missbrauch ihrer Daten zu schützen, bzw. schnell und besonnen auf einen solchen reagieren zu können (siehe auch ErwGr. 85).

Die Meldepflicht(en) in der DS-GVO sind u.a. in Artt. 33 und 34 der DS-GVO näher definiert. Eine Verletzung gegen diese Meldepflichten ist gem. Art. 83 Abs. 4 bußgeldbewährt und es drohen Bußgelder bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes. Bei den Meldepflichten gilt es zwischen der Meldepflicht an die Aufsichtsbehörde (Art. 33) und an den Betroffenen (Art. 34) zu unterscheiden.

9.9.1. Meldepflicht gegenüber der Aufsichtsbehörde

Kommentar:

Nach Art. 33 gilt, dass, wenn ein Verantwortlicher eine „Datenpanne“ feststellt, er diese unverzüglich (möglichst innerhalb von 72 Stunden) der für ihn zuständigen Aufsichtsbehörde (Art. 55) melden muss.

Durch die offene Formulierung in Art. 4 Nr. 12, die die „Verletzung personenbezogener Daten“ definiert, kann ziemlich schnell eine „Datenpanne“ angenommen werden, weshalb ein Verantwortlicher gut beraten ist, schnell und besonnen auf einen solchen Vorfall zu reagieren. . D. h. es ist angeraten, einen derartigen Vorfall ins Risikomanagement zu integrieren und ein Reaktions-Szenario geplant zu haben.

Anders als bspw. in § 42a BDSG sind in der DS-GVO keine „Kategorien“ von Daten benannt, die eine Meldepflicht auslösen. Dieses wiederum hat zur Konsequenz, dass theoretisch bei jeder „Datenpanne“ eine Meldepflicht an die Aufsichtsbehörde eintritt. Eine Ausnahme von der Meldepflicht besteht nur, wenn die „Datenpanne“ voraussichtlich nicht zu einem Risiko für die Betroffenen führt. Die Ermittlung, ob für den Betroffenen ein wie auch immer geartetes Risiko vorliegt und die diesbezügliche Beweislast, liegt beim Verantwortlichen. Erfolgt keine Meldung, so muss der Verantwortliche ggfs. nachweisen, aufgrund welcher Abwägungen dies nicht erfolgte. Hier ist daher eine sorgfältige Dokumentation der Abwägungsgründe erforderlich.

Falls die Meldung des Verantwortlichen nicht binnen 72 Stunden an die Aufsichtsbehörde erfolgt, ist der Verantwortliche verpflichtet, diese Verzögerung entsprechend zu begründen.

Für den Fall, dass ein Auftragsverarbeiter eine „Datenpanne“ feststellt, muss er diese ohne unangemessene Verzögerung dem Verantwortlichen melden. Versäumt er dieses oder verschweigt er die Datenpanne absichtlich, drohen ihm Sanktionen des Verantwortlichen (Auftraggebers).

Die Meldung der oder des Verantwortlichen an die Aufsichtsbehörde muss, den Regelungen der DS-GVO folgend, einige wesentliche Angaben beinhalten, welche der Aufsichtsbehörde eine Beurteilung des Falles erlauben. So muss diese Meldung an die gem. Art. 55 zuständige Behörde mindestens folgende Angaben beinhalten:

- eine Beschreibung der Art der Verletzung inkl. Angabe der Kategorien der Daten, Personen und Zahl der betroffenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder sonstigen Ansprechpartners für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls zur Eindämmung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, ist der Verantwortliche nach der DS-GVO verpflichtet, diese Informationen ohne unangemessene, weitere Verzögerung schrittweise der zuständigen Aufsichtsbehörde zur Verfügung zu stellen.

Ferner ist der Verantwortliche verpflichtet, etwaige „Datenpannen“ umfassend zu dokumentieren, indem er insbesondere alle „Fakten“ und Umstände des entsprechenden „Vorfalls“, die möglichen Auswirkungen auf die Betroffenen und die von ihm getroffenen Abhilfemaßnahmen beschreibt. Diese Dokumentation soll der Aufsichtsbehörde die Überprüfung der Einhaltung der rechtlichen Vorgaben ermöglichen (ErwGr. 85).

9.9.2. Meldepflicht gegenüber den Betroffenen

Kommentar:

Der Verantwortliche hat ferner die Pflicht, falls es wahrscheinlich ist, dass durch die „Datenpanne“ ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen besteht, diesen ohne

unangemessene Verzögerung von der Verletzung zu benachrichtigen. In dieser Benachrichtigung muss in klarer und einfacher Sprache die Art der (potentiellen) „Datenpanne“ beschrieben werden.

Ferner müssen hierin zumindest:

- die Kontaktdaten des DSB – des sonstigen Ansprechpartners,
- eine Beschreibung der wahrscheinlichen Folgen und
- eine Beschreibung der getroffenen Maßnahmen zur Behebung- / Minimierung des Schadens

enthalten sein.

Die Benachrichtigung der betroffenen Person gemäß Art. 34 Abs. 1 DS-GVO ist jedoch wiederum nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat, wozu bspw. die entsprechende (wirksame) Verschlüsselung der Daten gehören kann. Ferner entfällt eine Verpflichtung zur Meldung, wenn der für die Verarbeitung Verantwortliche durch Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 34 Abs. 1 aller Wahrscheinlichkeit nach nicht mehr besteht, oder dies mit einem unverhältnismäßigen Aufwand verbunden wäre. Für all dieses trägt er entsprechend Art. 5 Abs. 2 im Ernstfall die Beweislast.

In den Fällen, in denen die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre, muss er stattdessen die „Datenpanne“ öffentlich bekanntmachen (z. B. in der Presse veröffentlichen oder eine ähnliche Maßnahme treffen).

9.10. Verhältnis DS-GVO zu TMG / TKG

Kommentar:

Immer wieder kommt die Frage auf, wie das Verhältnis der Regelungen der DS-GVO gegenüber denen des TMG / TKG ist. Diese Frage stellt sich insbesondere bei Sachverhalten, in denen es um die „Rechtskonformität“ von Internetauftritten, Apps usw. geht. Doch wie man schon vermuten würde, ist die Rechtslage nicht ganz so eindeutig, wie es wünschenswert ist.

Wie vorstehend dargestellt, gehen zwar grundsätzlich die Regelungen der DS-GVO denen der nationalen Regelungen wie dem TMG / TKG vor (vgl. Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV)).

Daher dürften einige grundsätzliche Regelungen zum „Datenschutz“ in diesen Bereichen, wie im TMG die Pflicht zum Vorhalten einer „Datenschutzerklärung“ (§ 13 Abs. 2 TMG) obsolet werden und durch die Informationspflichten des Verarbeiters nach der DS-GVO ersetzt werden.

Zu beachten ist jedoch, dass einige Regelungen (bspw. im TMG) aufgrund von EU-Richtlinien wie etwa die „ePrivacy-Richtlinie“ 2002/58/EG in der Form der Ergänzungen der sog „Cookie-Richtlinie“ aus dem Jahre 2009 oder die Richtlinie 2000/31/EG (Richtlinie über den elektronischen Geschäftsverkehr), in das TKG / TMG übernommen wurden und somit nationales Recht darstellen.

Die DS-GVO enthält diesbezüglich die Regelung, dass diese Richtlinien (und die diesen RL zugrunde liegenden nationalen Gesetze) der DS-GVO vorgehen.

Wie sich aus Art. 95 erkennen lässt, ist eine grundsätzliche Revision und Harmonisierung der Richtlinie 2002/58/EG geplant. Es ist daher zu erwarten, dass die Regelungen dieser Richtlinien sich denen der DS-GVO annähern werden. Bis dahin kommt man nicht umhin, die geltenden Regelungen im Bereich „Telemedien“ entsprechend des jeweiligen individuellen Falles anzuwenden.

10. Datenschutzbeauftragter

Fundstelle in der DS-GVO:

- Art. 37 „Benennung eines Datenschutzbeauftragten“
- Art. 39 „Aufgaben des Datenschutzbeauftragten“

Kommentar:

Der Datenschutzbeauftragte (DSB) hat in Deutschland über die Jahre einen hohen Stellenwert erlangt. In anderen EU-Staaten ist er noch relativ unbekannt.

Durch die Bestellung eines Datenschutzbeauftragten erlangt ein Verantwortlicher in Deutschland gewisse „Privilegien“. So wird er als verantwortliche Stelle von gewissen Pflichten, wie etwa der Meldepflicht befreit. Die Regelungen zum Datenschutzbeauftragten finden sich in der DS-GVO in den Artt. 37 bis 39.

10.1. Bestellung

Kommentar:

Die Bestellung eines betrieblichen Datenschutzbeauftragten ist entsprechend Art. 37 DS-GVO für

- alle Behörden und öffentliche Einrichtungen (ausgenommen Gerichte)
- Unternehmen, zu deren Kerntätigkeit eine „umfangreiche regelmäßige und systematische Überwachung“ von Betroffenen gehört
- Unternehmen, zu deren Kerntätigkeit die umfangreiche Verarbeitung von besonderen Kategorien von Daten gehört, die in Art. 9 oder 10 DS-GVO beschrieben werden

verpflichtend. Dies ist dahin gehend nur konsequent, da Behörden etc. mit den meisten „Privilegien“ in der DS-GVO ausgestattet wurden. Behörden dürfen (je nach Größe), einen gemeinsamen Datenschutzbeauftragten bestellen. Auch eine Unternehmensgruppe kann einen gemeinsamen Datenschutzbeauftragten ernennen (Art. 37 Abs. 2 DS-GVO), sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann. Unter der Geltung der DS-GVO können somit Mehrfachbestellungen innerhalb eines Konzerns entfallen.

Ferner aber müssen entsprechend der Vorgaben der DS-GVO auch der Verantwortliche oder ein Auftragsverarbeiter einen Datenschutzbeauftragten bestellen, wenn die Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die eine umfangreiche, regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen (Profiling etc.) (Art. 37 Abs. 1 Lit. b), oder die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 […] besteht (Art. 37 Abs. 1 Lit. c). Damit müssen u.a. alle Verantwortlichen einen Datenschutzbeauftragten bestellen, zu deren Kerntätigkeit die Verarbeitung von Gesundheitsdaten oder genetischen Daten gehören.

Bei der Frage, was unter dem Begriff „Kerntätigkeit“ zu verstehen ist, muss auch ErwGr. 97 berücksichtigt werden. Gemäß ErwGr. 97 liegt eine Kerntätigkeit dann vor, wenn sich die Verarbeitung personenbezogener Daten auf die Haupttätigkeiten bezieht, nicht jedoch auf eine Nebentätigkeit. Entsprechend der Zielrichtung der DS-GVO ist dies so zu interpretieren, dass die Aktivität der Haupttätigkeit(en) im Umgang mit Daten bzw. Informationen liegen muss. Klassischerweise gehören zu diesen Aktivitäten insbesondere die

- Sammlung der Daten

- Auswertung der Daten
- Weitergabe/Übermittlung der Daten
- Weitergabe/Übermittlung der Ergebnisse der Auswertung.

Demgemäß gehört die Verwaltung des eigenen Personals nicht zu den Kerntätigkeiten eines Unternehmens, da diese Datenverarbeitung nur akzessorisch im Verhältnis zur eigentlichen Tätigkeit des Unternehmens anfällt. Erfolgt eine Datenverarbeitung hingegen als ein eigenständiges Leistungselement (z. B. bei einer Personal- oder Partnervermittlung), so ist diese Datenverarbeitung als Kerntätigkeit des Unternehmens anzusehen. Ob eine Kerntätigkeit im Hauptgeschäftsfeld oder lediglich in einem weiteren Betätigungsfeld des Verantwortlichen anfällt, ist dabei unerheblich.

Bzgl. des Gesundheitswesens sind die aus Verordnungen/Gesetzen resultierenden Anforderungen bei der Beurteilung der Kerntätigkeit zu berücksichtigen, z. B.:

- Dokumentationspflicht für Ärztinnen/Ärzte (§10 MBO-Ä[21], § 630f BGB[22])
- Dokumentationspflicht für Zahnärztinnen/Zahnärzte (§12 MBO[23], § 630f BGB[22])
- Dokumentationspflicht für Psychologischen Psychotherapeutinnen und Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeutinnen und Kinder- und Jugendlichenpsychotherapeuten (§9 MBO[24], § 630f BGB[22])
- Dokumentationspflicht für Pflegekräfte (jeweilige Berufsordnung für staatlich anerkannte Pflegeberufe z. B. [25] oder [26], § 630f BGB[22]).

Somit gehört es zur Kerntätigkeit der einen Patienten behandelnden Personengruppen, dass sie die Patientenbehandlung dokumentieren. Weder eine Diagnose noch eine Therapie ist ohne Ergebung der personenbezogenen Daten eines Patienten sowie deren Auswertung möglich, sodass auch aus dieser Sichtweise die Verarbeitung personenbezogener Daten zu den Kerntätigkeiten der einen Patienten behandelnden Personenkreise gehört.

Wie bisher kann der Datenschutzbeauftragte ein Beschäftigter des Verantwortlichen sein (interner Datenschutzbeauftragter) oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags (externer Datenschutzbeauftragter) erbringen.

Falls eine Bestellung nach dem Recht der Union oder der Mitgliedstaaten (nationale Öffnungsklausel) vorgeschrieben ist, müssen der Verantwortliche und ggfs. auch der Auftragsverarbeiter einen Datenschutzbeauftragten benennen (in Deutschland ist vorgesehen, dass die bisherigen Regelungen (§ 4f BDSG) beibehalten werden. Damit ändert sich im Grunde für Deutschland nichts. Während das BDSG gewisse Erleichterungen für Unternehmen mit bestelltem Datenschutzbeauftragten vorsieht,

[21] (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (2015) Online, zitiert am 2016-05-12; Verfügbar unter http://www.bundesaerztekammer.de/recht/berufsrecht/muster-berufsordnung-aerzte/muster-berufsordnung

[22] § 630f BGB „Dokumentation der Behandlung“. Online, zitiert am 2016-05-26; Verfügbar unter http://www.gesetze-im-internet.de/bgb/__630f.html

[23] Musterberufsordnung der Bundeszahnärztekammer (2014). Online, zitiert am 2016-05-26; Verfügbar unter http://www.bzaek.de/fileadmin/PDFs/recht/mbo.pdf

[24] Muster-Berufsordnung für die Psychologischen Psychotherapeutinnen und Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeutinnen und Kinder- und Jugendlichenpsychotherapeuten (2014) Online, zitiert am 2016-05-26; Verfügbar unter http://www.bptk.de/fileadmin/user_upload/Recht/Satzungen_und_Ordnungen/Musterberufsordnung_20140517.pdf

[25] Berufsordnung Land Berlin | Land Brandenburg (2009) Online, zitiert am 2016-05-26; Verfügbar unter http://www.deutscher-pflegerat.de/Downloads/Berufsordnungen/LPR-B_BB-Berufsordnung2010.pdf

[26] Berufsordnung des Dachverbandes der Pflegeorganisationen Rheinland-Pfalz e.V. (2006) Online, zitiert am 2016-05-26; Verfügbar unter http://www.dpo-rlp.de/berufsordnung.html

bietet die DS-GVO hier keinerlei Anreize für Unternehmen. Daher gibt es ohne gesetzliche Anforderung für ein Unternehmen keinen rationalen Grund, auf freiwilliger Basis einen Datenschutzbeauftragten zu bestellen.

10.2. Vorgaben für die Bestellung / Tätigkeit eines DSB

Kommentar:

Der Datenschutzbeauftragte muss eine entsprechende berufliche Qualifikation und entsprechendes Fachwissen insbesondere auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis aufweisen. Hinsichtlich des Fachwissens ist ErwGr. 97 zu entnehmen: „Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten“. Damit muss das Fachwissen selbstverständlich auch das Wissen der Domäne, in welcher der Datenschutzbeauftragte tätig ist (z. B. Bank oder Gesundheitswesen), umfassen, zugleich ist die Beurteilung der tiefe der Kenntnisse vom Risiko der Datenverarbeitung abhängig, sodass ein Datenschutzbeauftragter im Maschinenbau bzgl. der notwendigen Kenntnisse anders zu beurteilen ist als ein Datenschutzbeauftragter in Bereichen, die besondere Kategorien von Daten entsprechend Art. 9 DS-GVO verarbeiten.

Wie bisher ist die Unabhängigkeit des Datenschutzbeauftragten zwingend notwendig, desgleichen das er seine Aufgaben in vollständiger Unabhängigkeit ausüben kann

Dem Verantwortlichen / Auftragsverarbeiter obliegt die Pflicht, die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.

Hinsichtlich der Stellung des DSB hat sich gegenüber der heutigen Rechtslage in Deutschland wenig geändert. So muss bspw. stets sichergestellt sein, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird, er entsprechende Ressourcen zur Verfügung hat, um seine Aufgaben (Art. 39) wahrzunehmen und sein Fachwissen aktuell zu halten bzw. sich neues Wissen anzueignen. Ferner muss es ihm, zur Erfüllung seiner Aufgaben möglich sein, Zugang zu den Verfahren zu erhalten. Es muss sichergestellt sein, dass er seine Funktion als Hauptansprechpartner für Betroffene in ausreichendem Maße ausüben und weisungsfrei agieren kann. Er darf nicht wegen seiner Tätigkeit als Datenschutzbeauftragter abberufen oder benachteiligt werden. Allerdings ist der Kündigungsschutz in der DS-GVO im Gegensatz zum BDSG nicht verankert.

Die DS-GVO weist dem DSB ein Berichtsrecht wie auch eine Berichtspflicht gegenüber der höchsten Managementebene, also dem Verantwortlichen, zu. Lediglich die Pflicht zur unmittelbaren Unterstellung unter die Leitung der Stelle entfällt künftig.

Entsprechend dem Recht der Union oder der Mitgliedstaaten ist der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden (nationale Öffnungsklausel).

Neben seiner Tätigkeit als Datenschutzbeauftragter kann er weitere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche / Auftragsverarbeiter muss jedoch wie bisher sicherstellen, dass es bei der Erfüllung dieser Aufgaben und Pflichten nicht zu Interessenkonflikten mit den Pflichten / Aufgaben, die dem Datenschutzbeauftragten obliegen, kommt.

10.3. Aufgaben des DSB

Kommentar:

Nach Art. 37 obliegen dem Datenschutzbeauftragten folgende, nicht abschließend aufgezählte Aufgaben:

- Die Überwachung der Einhaltung der geltenden Datenschutzvorschriften;
- die Unterrichtung und Beratung des Verantwortlichen oder Auftragsverarbeiters, inkl. der Beschäftigten, die personenbezogene Daten verarbeiten, hinsichtlich ihrer Pflichten entsprechend der geltenden Datenschutzvorschriften; einschließlich der Zuweisung von Zuständigkeiten:
- der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- der Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;
- die Zusammenarbeit mit der Aufsichtsbehörde.

Ferner unterstützt er den oder die Verantwortlichen / Auftragsverarbeiter bei der Erfüllung der ihm bzw. ihnen obliegenden Meldepflichten.

11. Datenschutz und Berufsgeheimnisträger

11.1. Arzt als Auftragsverarbeiter

Kommentar:

Entsprechend Art. 4 Abs. 8 DS-GVO ist ein Auftragsverarbeiter „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet". Art. 28 Abs. 3 Lit. a DS-GVO verlangt jedoch, dass ein Auftragsverarbeiter Daten „nur auf dokumentierte Weisung des Verantwortlichen" verarbeitet, d. h. nur entsprechend der Weisung des Auftraggebers die Daten verarbeiten darf.

Entsprechend § 2 Abs. 1 Muster-Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte[27] (MBO-Ä) sowie der Umsetzungen in die jeweiligen Landesordnungen dürfen sie „keine Grundsätze anerkennen und keine Vorschriften oder Anweisungen beachten, die mit ihren Aufgaben nicht vereinbar sind oder deren Befolgung sie nicht verantworten können"[27]. Damit kann ein Arzt nicht als Auftragsverarbeiter für einen anderen Arzt tätig werden, da er im Zweifel gegen die Anweisung des anderen Arztes verstoßen muss.

Entsprechend Erwägungsgrund 53 soll die DS-GVO „harmonisierte Bedingungen für die Verarbeitung besonderer Kategorien personenbezogener Gesundheitsdaten im Hinblick auf bestimmte Erfordernisse" schaffen. Insbesondere wenn die Verarbeitung für „gesundheitsbezogene Zwecke von Personen durchgeführt wird, die gemäß einer rechtlichen Verpflichtung dem Berufsgeheimnis unterliegen".

D. h. die DS-GVO soll auch für dem Berufsgeheimnis unterliegende medizinische Personenkreise harmonisierte datenschutzrechtliche Rahmenbedingungen in Europa schaffen.

Da Regelungen zum Berufsgeheimnis jedoch der nationalen Gesetzgebungskompetenz unterliegen, finden sich in der DS-GVO selbst keine diesbezüglichen Aussagen, sondern es wird an den jeweiligen Stellen an den nationalen Gesetzgeber verwiesen. Z. B. wird dem nationalen Gesetzgeber in Art. 90 DS-GVO aufgegeben zu regeln, wie nationale Datenschutz-Aufsichtsbehörden Zugriff auf Daten bei Berufsgeheimnisträgern erhalten können.

11.2. Gemeinsame Verarbeitung

Kommentar:

Häufig kommt es vor, dass zwei oder mehr ärztlich geleitete Institutionen einen Patienten gemeinsam behandeln, z. B. im Rahmen einer onkologischen Behandlung oder der Sterbebegleitung durch ein Hospiz. Hier arbeitet ein Krankenhaus (oder ggfs. auch mehrere) mit niedergelassenen Ärzten gemeinsam an der Behandlung. Wie in Kapitel 11.1 besprochen wurde, ist die Konstellation einer Auftragsverarbeitung hier nicht möglich.

Hier bietet sich an, als „gemeinsam für die Verarbeitung Verantwortliche" entsprechend Art. 26 DS-GVO aufzutreten: i.d.R. spricht man sich bzgl. der Patientenbehandlung ab und legt gemeinsam das Vorgehen fest; in einem Kooperationsvertrag ist geregelt, wer welche Verpflichtungen hat. Künftig müsste in diesen Kooperationsverträgen festgelegt werden, wer welchen Pflichten der DS-GVO nachkommt, sodass die diesbezüglichen Anforderungen der DS-GVO erfüllt werden.

[27] Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (2015) Online, zitiert am 2016-05-12; Verfügbar unter http://www.bundesaerztekammer.de/recht/berufsrecht/muster-berufsordnung-aerzte/muster-berufsordnung/

Weiterhin müssen die Informationssysteme im Krankenhaus wie auch im niedergelassenem Umfeld so angepasst werden, dass ein Zugriff nur auf gemeinsam behandelte Patienten für die jeweils berechtigten (externen) Partner ermöglicht wird.

12. Forschung

Kommentar:

Der Begriff der „Forschung“ selbst ist in der DS-GVO nicht definiert. Die Erwägungsgründe geben aber eine Vorstellung, was der europäische Gesetzgeber darunter versteht, z. B.

- Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden (Erwägungsgründe 53, 159)
- Klinische Prüfungen (Erwägungsgrund 156)
- Register (Erwägungsgrund 157)
- Verbesserung der Lebensqualität zahlreicher Menschen (Erwägungsgrund 157)
- Verbesserung der Effizienz der Sozialdienste (Erwägungsgrund 157)
- Grundlagenforschung (Erwägungsgrund 159)
- Angewandte Forschung (Erwägungsgrund 159)
- Privat finanzierte Forschung (Erwägungsgrund 159).

12.1. Erlaubnistatbestand

Kommentar:

Grundsätzlich ist für jegliche Verarbeitung personenbezogener oder personenbeziehbarer Daten ein Erlaubnistatbestand erforderlich. Gemäß Art. 9 Abs. 1 ist jegliche Verarbeitung besonderer Kategorien personenbezogener Daten verboten (und damit auch die Verarbeitung zu Forschungszwecken), außer ein in Art. 9 Abs. 2 genannter Umstand trifft zu.

12.1.1. Verarbeitung mit Einwilligung des Betroffenen

Kommentar:

Gemäß Art. 9 Abs. 2 Lit. a ist eine Verarbeitung besonderer Kategorien personenbezogener Daten gestattet, wenn

a) die betroffene Person einwilligt und
b) Unionsrecht oder das Recht von Mitgliedstaaten die Verarbeitung nicht verbieten.

Für eine wirksame Einwilligung müssen die Vorgaben der DS-GVO eingehalten werden (siehe Kapitel 7).

12.1.2. Verarbeitung ohne Einwilligung des Betroffenen

Kommentar:

Hinsichtlich der Nutzung besonderer Kategorien personenbezogener Daten findet sich in Art. 9 Abs. 2 Lit. j ein datenschutzrechtlicher Erlaubnistatbestand: „die Verarbeitung ist

- auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats,
- das in angemessenem Verhältnis zu dem verfolgten Ziel steht,
- den Wesensgehalt des Rechts auf Datenschutz wahrt und
- angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht,
- für
    - im öffentlichen Interesse liegende Archivzwecke,
    - für wissenschaftliche oder
    - historische Forschungszwecke oder

- für statistische Zwecke

gemäß Artikel 89 Absatz 1 erforderlich.

Somit können besondere Kategorien personenbezogener Daten zu „wissenschaftlichen Forschungszwecken“ genutzt werden, wenn fünf Bedingungen erfüllt sind:

a) ein nationales oder europäisches Recht für die Nutzung existiert,
b) dieses Recht steht im angemessenem Verhältnis zum verfolgten (Forschungs-) Ziel,
c) dieses Recht wahrt die datenschutzrechtlichen Anforderungen der DS-GVO,
d) das Gesetz sieht spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vor und
e) die Verarbeitung der Daten ist erforderlich.

Sind diese Bedingungen erfüllt, so müssen weiterhin die Vorgaben in Art. 89 Abs. 1 berücksichtigt werden: „Die Verarbeitung zu

- im öffentlichen Interesse liegenden Archivzwecken,
- zu wissenschaftlichen oder historischen Forschungszwecken oder
- zu statistischen Zwecken

unterliegt

- geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung.

Mit diesen Garantien wird sichergestellt, dass

- technische und organisatorische Maßnahmen bestehen,
- mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.“

D. h. jedes Forschungsvorhaben muss den Vorgaben der DS-GVO genügen, insbesondere muss es auch

- den Grundsätzen der Verarbeitung genügen (Kapitel II),
- die Betroffenenrechte wahren (Kapitel III) und
- die Sicherheit der Verarbeitung gewährleisten (Kapitel IV).

Insbesondere hat die betroffene Person gemäß Art. 21 Abs. 6 das Recht, der Nutzung „sie betreffender personenbezogener Daten, die zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Artikel 89 Absatz 1“ verwendet werden sollen, zu widersprechen. Es sei denn, die Verarbeitung erfolgt im „öffentlichen Interesse“ (siehe Kapitel 6.8).

12.2. Zweckanpassung

Kommentar:

Mitunter werden für Forschungszwecke personenbezogene Daten benötigt, die ursprünglich für einen anderen Zweck erhoben wurden. Art. 5 Abs. 1 Lit. b schreibt hier „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken“.

Somit können unter den bereits beschriebenen Voraussetzungen von Art. 89 Abs. 1 (siehe Kapitel 12.1.2) z. B. Daten der Routineversorgung grundsätzlich für wissenschaftliche Forschungsvorhaben genutzt werden, wenn ein Erlaubnistatbestand (siehe Kapitel 12.1) vorhanden ist.

Entsprechend Art. 14 Abs. 4 DS-GVO muss der Betroffene vor Beginn der Weiterverarbeitung der Daten „Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen" gemäß Art. 14 Abs. 2 zur Verfügung stellen. D. h. das z. B. der Patient vor Verwendung der Daten der Routineversorgung zu einem Forschungszweck grundsätzlich informiert werden muss. Es sei denn, ein Ausnahmetatbestand gemäß Art. 14 Abs. 5 trifft zu. Ist Letzteres der Fall muss der Verzicht der Information des Betroffenen gemäß Art. 5 dokumentiert werden, damit bei einer Überprüfung die Entscheidungsfindung bzgl. des Informationsverzichts des Betroffenen dargestellt und von den Prüfern nachvollzogen und beurteilt werden kann.

12.3. Anonyme Daten

Kommentar:

Wenngleich in den Erwägungsgründen erwähnt wird, dass für anonyme Daten die Grundsätze des Datenschutzes nicht gelten sollten (z. B. Erwägungsgrund 26), findet sich im Gegensatz zum BDSG in der DS-GVO selbst keine Definition bzgl. anonymer Daten. Die Begrifflichkeit der anonymen Daten kann somit nur indirekt aus den Erwägungsgründen abgeleitet werden.

Da die Grundsätze des Datenschutzes nicht gelten, kann es sich bei anonymen Daten nicht um pseudonyme Daten oder andere personenbezogene Daten gemäß Art. 4 Abs. 1 handeln. Somit besteht hier eine Abgrenzung zu den personenbezogenen oder personenbeziehbaren Daten.

Gemäß Erwägungsgrund 26 sind anonyme Daten Informationen, „die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann". D. h. anonyme Daten dürfen keinen Personenbezug beinhalten. Somit sind anonyme Daten im Sinne der DS-GVO Daten, die wir in Deutschland bisher mit dem Begriff „absolut anonym" klassifizierten.

Dieses Verständnis bzgl. der Begrifflichkeit „anonyme Daten" entspricht auch dem bisherigen europäischem Verständnis, wie es beispielsweise von der Artikel-29-Datenschutzgruppe 2014 dargestellt wurde[6]. Werden personenbezogene Daten anonymisiert, so stellt dies eine Weiterverarbeitung[6] dar, für die selbstverständlich zunächst einmal die Erfordernisse der DS-GVO gelten. D. h. für die Anonymisierung ist insbesondere auch ein Erlaubnistatbestand (siehe Kapitel 12.1 bzw. Kapitel 7) erforderlich.

13. Sanktionen / Strafregelungen

13.1. Bußgelder

Fundstelle in der DS-GVO:

- Art. 83 „Allgemeine Bedingungen für die Verhängung von Geldbußen“

Kommentar:

§ 43 BDSG kennt Bußgelder von bis zu 50.0000 Euro bzw. bis zu 300.000 Euro. Die DS-GVO geht weit darüber hinaus und sieht Bußgelder von bis zu 20 Mio. Euro oder bis zu 4 % des letzten weltweiten Jahresumsatzes vor.

Im Einzelnen sieht die DS-GVO drei Abstufungen vor:

1) Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes (Art. 83 Abs. 4)
   Z. B. bei Verstoß gegen
   - Art. 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen)
   - Art. 28 (Auftragsverarbeiter)
   - Art. 29 (Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters)
   - Art. 30 (Verzeichnis von Verarbeitungstätigkeiten)
   - Art. 31 (Zusammenarbeit mit der Aufsichtsbehörde)
   - Art. 32 (Sicherheit der Verarbeitung)
   - Artt. 33 u. 34 (Meldung von Datenpannen an Aufsichtsbehörde und Betroffenen)
   - Art. 35 (Datenschutzfolgenabschätzung)
   - Artt. 36 bis 39 (Datenschutzbeauftragter)
2) Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes (Art. 83. Abs. 5)
   Z. B. bei Verstoß gegen
   - Artt. 5, 6, 7, 9 (fehlende oder fehlerhaft eingeholte Einwilligung)
   - Artt. 12-22 (Verstoß gegen die Rechte der/des Betroffenen)
   - Artt. 44 bis 49 (Unrechtmäßige Übermittlung in ein Drittland oder int. Organisation)
   - Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde
3) Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes (Art. 83. Abs. 6)
   Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Art. 58 Abs. 2

Ein großer Unterschied in den Bußgeld-Regelungen besteht, abgesehen von der Höhe, u.a. in den Vorgaben bzgl. der Vergabe von Bußgeldern. In §43 Abs. 3 BDSG steht „Die Ordnungswidrigkeit kann...“, in Art. 83 Abs. 2 ist die Formulierung „Geldbußen werden...“ zu finden. Wenn im Falle des BDSG eine Aufsichtsbehörde noch entscheiden konnte, ob ein Bußgeld verhangen wird, so muss in Zukunft eine Aufsichtsbehörde ein Bußgeld verhängen. Lediglich bzgl. der Höhe des Bußgeldes besitzt die Aufsichtsbehörde noch einen gewissen Spielraum. Der Spielraum ist allerdings eingeschränkt:

1) Die Höhe der Geldbuße bei einem Verstoß muss sich „europäisch“ einordnen. D. h. für einen Verstoß muss in allen Ländern ein den Umständen entsprechendes, einheitliches Bußgeld

verhangen werden. Dabei muss natürlich auch die Wirtschaftslage berücksichtigt werden: ein Bürger wird voraussichtlich in allen Ländern ein wirtschaftlich gleich großes Bußgeld erhalten, welches sich vom absoluten Betrag jedoch von Land zu Land unterscheiden kann. Ein globales Unternehmen hingegen wird voraussichtlich nach seiner Gesamt-Wirtschaftsleistung beurteilt, unabhängig von der einzelnen Leistung im Land, in welchem das Bußgeld verhangen wird. Die Aufsichtsbehörden planen hier einen Bußgeldkatalog zu erstellen, sodass die Einordnung erleichtert wird.

2) In Art. 83 Abs. 2 Lit. a-k schreibt der europäische Gesetzgeber den Aufsichtsbehörden vor, was bei der Verhängung eines Bußgeldes berücksichtigt werden muss. Insbesondere gehören hierzu:
   a. Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
   b. Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters
   c. etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters
   d. Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind.

   Somit steht zu erwarten, dass Verstöße bei der Verarbeitung besonderer Kategorien personenbezogener Daten wie beispielsweise Gesundheitsdaten höhere Bußgelder nach sich ziehen als bei „normalen“ personenbezogenen Daten.

13.2. Sanktionen der Mitgliedstaaten

Fundstelle in der DS-GVO:

- Art. 84 „Sanktionen“

Kommentar:

Die Mitgliedsstaaten werden beauftragt, weitere Strafvorschriften einzuführen. Darunter fallen z. B. auch die strafrechtlichen Sanktionen, wie sie aktuell in § 44 BDSG geregelt sind.

14. Empfehlungen

1. Budgetplanung beim Datenschutzbeauftragter anpassen
   a) Der Datenschutzbeauftragte muss Fortbildungen besuchen, um sich einen Überblick zu verschaffen und das Wissen anzueignen, was konkret an Umsetzungen im Unternehmen ansteht
   b) Es muss neue Literatur zur Datenschutz-Grundverordnung angeschafft werden
2. Ggfs. externe Beratung einholen
3. Anpassung der eingesetzten IT-Systeme beauftragen
   a) Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
   b) Recht auf Datenübertragbarkeit
   c) Recht auf Löschung / „Vergessenwerden“
   d) Einwilligung mit Symbolen: ggfs. Maschinenlesbarkeit notwendig
4. Anpassung im Unternehmen
   a) Auftragsdatenverarbeitungsverträge überarbeiten
   b) IT-Sicherheit prüfen: Steht eine dem „Stand der Technik“[28] entsprechende IT-Landschaft zur Verfügung?
   c) Einwilligung anpassen (Cave: nur eine Einwilligung, welche den Anforderungen der DS-GVO genügt, kann nach Eintreten der Geltung der DS-GVO weiterhin als Legitimationsgrundlage für eine Datenverarbeitung im Sinne von Art. 4 Abs. 2 DS-GVO gelten.)
   d) Auskunftsansprüche Betroffener berücksichtigen, z. B.
      - Verarbeitungszwecke müssen angegeben werden
      - Rechtsgrundlage, aufgrund welcher die Verarbeitung erfolgt, muss angegeben werden
      - Speicherfristen beachten
      - insbesondere Benachrichtigung Betroffener bei Aufhebung einer Sperrung
   e) Information des Betroffenen an neue Anforderungen anpassen (z. B. Symbole ergänzen)
   f) Datenschutz-Folgenabschätzung in den Prozessmanagement-Workflow integrieren
   g) Workflow bzgl. Datenverlust / Datenleck anpassen; bei einer Meldepflicht innerhalb 72 Stunden sollten Zuständige benannt und Entscheidungshilfen vorbereitet werden.

[28] Begrifflichkeit „Stand der Technik“ siehe auch

- BVerfG Urt. v. 08.08.1978 Az.: 2 BvL 8/77. Online, zitiert am 2016-05-13; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Text=2%20BvL%208/77
- §3 Abs. 2 Patentgesetz. Online, zitiert am 2016-05-13; Verfügbar unter http://www.gesetze-im-internet.de/patg/__3.html
- DIN EN 45020:2007-03. Normung und damit zusammenhängende Tätigkeiten - Allgemeine Begriffe.

15. Literatur

15.1. Bücher

- Gierschmann S, Schlender K, Stentzel R, Veil V. (Hrsg.) Kommentar EU-Datenschutz-Grundverordnung. Bundesanzeiger Verlag. ISBN 3846206385
  (angekündigt August 2016)
- Gola P. (Hrsg.) DS-GVO: Datenschutz-Grundverordnung (Gelbe Erläuterungsbücher). Verlag C.H.Beck. ISBN 3406695434
  (angekündigt Dezember 2016)
- Kazemi R. Die Datenschutz-Grundverordnung in der anwaltlichen Beratungspraxis. Deutscher Anwaltverlag. ISBN 3824014505
  (angekündigt Juni 2016)
- Paal B. Datenschutz-Grundverordnung (Beck'sche Kompakt-Kommentare) Verlag C.H. Beck. ISBN 3406695701
  (angekündigt Oktober 2016)
- Raab J. (2015) Die Harmonisierung des einfachgesetzlichen Datenschutzes: Von der umsetzungsdefizitären Datenschutzrichtlinie 95/46/EG zur Datenschutz-Grundverordnung. Lit. Verlag. ISBN 978-3643131805
- Roßnagel A. (Hrsg.) Europäische Datenschutz-Grundverordnung - Vorrang des Unionsrechts/Anwendbarkeit des nationalen Rechts. Nomos Verlag. ISBN 384873074X
  (angekündigt September 2016)
- Schantz P, Wolff HA. Das neue Datenschutzrecht: Die Datenschutz-Grundverordnung in der Praxis. Verlag C.H.Beck. ISBN 340669649X.
  (angekündigt Dezember 2016)

15.2. Juristische Fach-Zeitschriften

2016

- Albrecht JP. (2016) Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung. CR: 88-98
- Becker T. (2016) EU-Datenschutz-Grundverordnung - Anforderungen an Unternehmen und Datenschutzbeauftragte. ITRB: 107-108
- Boehm F, Andrees M. (2016) Zur Vereinbarkeit der Vorratsdatenspeicherung mit europäischem Recht - Bewertung der generellen Speicherpflicht nach EuGH und EGMR Rechtsprechung. CR: 146-154
- Buchner B. (2016) Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO.DuD: 155-161
- Däubler W. (2013) Datenschutz wird europäisch. AiB: 26-31
- Dieterich T. (2016) Rechtsdurchsetzungsmöglichkeiten der DS-GVO - Einheitlicher Rechtsrahmen führt nicht zwangsläufig zu einheitlicher Rechtsanwendung. ZD: 260266
- Eckhardt J, Kramer R. (2016) Auftragsdatenverarbeitung beim Einsatz von Persönlichkeitsanalysetools. DuD: 144-149
- Faust S, Spittka J, Wybitul T. (2016) Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz. ZD: 120-125
- Franck L. (2016) Datensicherheit als datenschutzrechtliche Anforderung. CR: 238-240

- Gierschmann S. (2016) Was „bringt“ deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt. ZD: 51-55
- Gola P. (2016) Verbandsklagen – ein neues Schwert des Datenschutzes? RDV: 17-21
- Gola P, Lepperhoff N. (2016) Reichweite des Haushalts- und Familienprivilegs bei der Datenverarbeitung - Aufnahme und Umfang der Ausnahmeregelung in der DS-GVO. ZD: 9-12
- Gola P, Pötters S, Thüsing G. (2016) Art. 82 DSGVO: Öffnungsklausel für nationale Regelungen zum Beschäftigtendatenschutz – Warum der deutsche Gesetzgeber jetzt handeln muss. RDV: 57-61
- Härting N. (2016)Auftragsverarbeitung nach der DSGVO. ITRB: 137-140
- Halfmeier A. (2016) Die neue Datenschutzverbandsklage. NJW: 1126-1129
- Hayen RP. (2016) „Der Kampf lohnt sich!“ - Fragen von der Redaktion. AiB: 32-33
- Jaspers A, Reif Y. (2016) Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben. RDV: 61-68
- Kartheuser I, Schmitt F. (2016) Der Niederlassungsbegriff und seine praktischen Auswirkungen Anwendbarkeit des Datenschutzrechts eines Mitgliedstaats auf ausländische EU-Gesellschaften. ZD:155-159
- Kraska S. (2016) Auswirkungen der EU-Datenschutzgrundverordnung. ZD-Aktuell: 04173
- Lepperhoff N, Müthlein T. (2016) Datenschutz-Grundverordnung: Neue Vorschriften – auch für die Security! kes: 54-63
- Lotz B, Wendle J. (2016) Datensicherheit als datenschutzrechtliche Anforderung: Zur Frage der Abdingbarkeit des § 9 BDSG. CR: 31-36
- Molnár-Gábor F, Korbel JO. (2016) Verarbeitung von Patientendaten in der Cloud - Die Freiheit translationaler Forschung und der Datenschutz in Europa. ZD: 274-281
- Müthlein T. (2016) ADV 5.0 - Neugestaltung der Auftragsdatenverarbeitung in Deutschland. RDV: 7487
- Peifer KN. (2016) Beseitigungsansprüche im digitalen Äußerungsrecht - Ausweitung der Pflichten des Erstverbreiters. NJW: 23-25
- Pollmann M, Kipker DK. (2016) Informierte Einwilligung in der Online-Welt. DuD: 378-381
- Richter P. (2016) Instrumente zwischen rechtlicher Steuerung und technischer Entwicklung. DuD: 89-93
- Ronellenfitsch M. (2016) Kohärenz und Vielfalt. DuD: 357-359
- Schmitz B, von Dall’Armi J. (2016) Standardvertragsklauseln – heute und morgen: Eine Alternative für den Datentransfer in Drittländer? ZD: 217-223
- Schwartmann R, Weiss S. (2016) Ko-Regulierung vor einer neuen Blüte – Verhaltensregelungen und Zertifizierungsverfahren nach der Datenschutzgrundverordnung (Teil 1). RDV: 68-73
- Sörup T. (2016) Gestaltungsvorschläge zur Umsetzung der Informationspflichten der DS-GVO im Beschäftigungskontext. ArbRAktuell: 207-213
- Sörup T, Marquardt S. (2016) Auswirkungen der EU-Datenschutzgrundverordnung auf die Datenverarbeitung im Beschäftigungskontext. ArbRAktuell: 103-106
- Taeger J. (2016) Scoring in Deutschland nach der EU-Datenschutzgrundverordnung. ZRP: 72-75
- Ulmer CD, Rath M. (2016) Die neue EU-Datenschutz-Grundverordnung. CCZ: 142-144
- Werkmeister C, Brandt E. (2016) Datenschutzrechtliche Herausforderungen für Big Data. CR: 233-238

- Wybitul T. (2016) Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte? Anpassungsbedarf bei Beschäftigtendatenschutz und Betriebsvereinbarungen. ZD: 203-208
- Wybitul T, Pötters S (2016) Der neue Datenschutz am Arbeitsplatz. RDV 2016:10-16

2015

- Ashkar D. (2015) Durchsetzung und Sanktionierung des Datenschutzrechts nach den Entwürfen der Datenschutz-Grundverordnung. DuD: 796-800
- Bender S, Elias P. (2015) Forschung mit Big Data – die europäische Perspektive. Bundesgesundheitsbl 58: 799–805
- Bräutigam P, Schmidt-Wudy F. (2015) Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung. CR: 56-63
- Bretthauer S, Krempel E, Birnstill P. (2015) Intelligente Videoüberwachung in Kranken- und Pflegeeinrichtungen von morgen. CR: 239-245
- Brink S, Eckhardt J. (2015) Wann ist ein Datum ein personenbezogenes Datum? Anwendungsbereich des Datenschutzrechts.ZD: 205-212
- Brisch K, Pieper F. (2015) Das Kriterium der „Bestimmbarkeit“ bei Big Data-Analyseverfahren - Anonymisierung, Vernunft und rechtliche Absicherung bei Datenübermittlungen. CR: 724-729
- Ehmann E. (2015) Der weitere Weg zur Datenschutzgrundverordnung - Näher am Erfolg, als viele glauben? ZD: 6-12
- Gerhard T. (2015) Vereinbarkeit einer Verbandsklage im Datenschutzrecht mit Unionsrecht. CR: 338-344
- Grau T, Schaut A. (2015) Neue Spielregeln für die Verwendung von Bilddateien von Arbeitnehmern. NZA: 981-984
- Härting N, Schneider J. (2015)Das Ende des Datenschutzes – es lebe die Privatsphäre. CR: 819-827
- Karg M. (2015) Anonymität, Pseudonyme und Personenbezug revisited? DuD: 520-526
- Keppeler LM. (2015) Was bleibt vom TMG-Datenschutz nach der DS-GVO? Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz. MMR: 779-783
- Kieselmann O, Kopal N, Wacker A. (2015) „Löschen“ im Internet - Ein neuer Ansatz für die technische Unterstützung des Rechts auf Löschen. DuD: 31-36
- Knopp M. (2015) Dürfen juristische Personen zum betrieblichen Datenschutzbeauftragten bestellt werden? DuD: 98-102
- Mester BA. (2015) EU-Datenschutzgrundverordnung. DuD: 822
- Nguyen AM. (2015) Die zukünftige Datenschutzaufsicht in Europa - Anregungen für den Trilog zu Kap. VI bis VII der DS-GVO. ZD: 265-270
- Petri T. (2015) Auftragsdatenverarbeitung – heute und morgen - Reformüberlegungen zur Neuordnung des Europäischen Datenschutzrechts. ZD: 305-309
- Preuß T. (2015) Das Datenschutzrecht der Religionsgesellschaften - Eine Untersuchung de lege lata und de lege ferendanach Inkrafttreten der DS-GVO. ZD: 217-225
- Richter P. (2015) Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO. DuD: 735-740
- Roßnagel A, Nebel M, Richter P. (2015) Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO. ZD: 455-460

- Veil W. (2015) DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme. ZD: 347-353
- Wybitul T, Sörup T, Pötters S. (2016) Betriebsvereinbarungen und § 32 BDSG: Wie geht es nach der DS-GVO weiter? Handlungsempfehlungen für Unternehmen und Betriebsräte. ZD: 559-564
- Zikesch P, Kramer R. (2015) Die DS-GVO und das Berufsrecht der Rechtsanwälte, Steuerberater und Wirtschaftsprüfer - Datenschutz bei freien Berufen. ZD: 565-570

2014

- Dorner M. (2014) Big Data und „Dateneigentum" - Grundfragen des modernen Daten- und Informationshandels. CR: 617-628
- Eckhardt J, Kramer R. (2014) Auftragsdatenverarbeitung - Datenschutzrechtliches Gestaltungselement zwischen Recht und Technik. DuD: 147-152
- Katko P, Babaei-Beigi A. (2014) Accountability statt Einwilligung? Führt Big Data zum Paradigmenwechsel im Datenschutz? MMR: 360-364
- Koós C, Englisch B. (2014) Eine „neue" Auftragsdatenverarbeitung - Gegenüberstellung der aktuellen Rechtslage und der DS-GVO in der Fassung des LIBE-Entwurfs. ZD: 276-285
- Langhanke C. (2014) Datenschutz in der Schweiz - Reichweite der europarechtlichen Vorgaben. ZD: 621-625
- Monreal M. (2014) Der für die Verarbeitung Verantwortliche„ – das unbekannte Wesen des deutschen Datenschutzrechts. ZD: 611-616
- Richter P. (2014) Ein anonymes Impressum? Profile in sozialen Netzwerken zwischen Anbieterkennzeichnung und Datenschutz. MMR: 517-521
- Schneider J, Härting N. (2014) Datenschutz in Europa – Plädoyer für einen Neubeginn: Zehn „Navigationsempfehlungen", damit das EU-Datenschutzrecht internettauglich und effektiv wird. CR: 306-312
- Sydow G, Kring M. (2014) Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug - Konkurrierende Leitbilder für den europäischen Rechtsrahmen. ZD: 271-276
- Weichert, T. (2014) Scoring in Zeiten von Big Data. ZRP: 168-171

2013

- Dehmel S, Hullen N. (2013) Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa? Konkrete Auswirkungen der DS-GVO auf Wirtschaft, Unternehmen und Verbraucher. ZD: 147-153
- Eckhardt J, Kramer R. (2013) DS-GVO – Diskussionspunkte aus der Praxis. DuD: 287-294
- Eckhardt J, Kramer R, Mester BA. (2013) Auswirkungen der geplanten EU-DS-GVO auf den deutschen Datenschutz. DuD: 623-630
- Gerling S, Gerling RW. (2013) Wie realistisch ist ein „Recht auf Vergessenwerden"? DuD: 445-446
- Härting N. (2013) Anonymität und Pseudonymität im Datenschutzrecht. NJW: 2065-2071
- Jandt S, Kieselmann O, Wacker A. (2013) Recht auf Vergessen im Internet - Diskrepanz zwischen rechtlicher Zielsetzung und technischer Realisierbarkeit? DuD: 235-241
- Kamp M, Rost M. (2013) Kritik an der Einwilligung - Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen. DuD: 80-84
- Klar M. (2013) Räumliche Anwendbarkeit des (europäischen) Datenschutzrechts - Ein Vergleich am Beispiel von Satelliten-, Luft- und Panoramastraßenaufnahmen. ZD: 109-115
- Kodde C. (2013) Die „Pflicht zu Vergessen" - „Recht auf Vergessenwerden" und Löschung in BDSG und DS-GVO. ZD: 115-118

- König T. (2013) Zur Möglichkeit einer sektoralen Datenschutzkontrolle nach dem Entwurf der EU-Grundverordnung. DuD: 101-103
- Kranig T. (2013) Zuständigkeit der Datenschutzaufsichtsbehörden - Feststellung des Status quo mit Ausblick auf die DS-GVO. ZD: 550-557
- Quiring-Kock G. (2013) Entwurf EU-Verordnung über elektronische Identifizierung und Vertrauensdienste. DuD: 20-24
- Schüßler L, Zöll O. (2013) EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz. DuD: 639-643
- Seifert B. (2013) Neue Regeln für die Videoüberwachung? Visuelle Kontrolle im Entwurf der EU-Datenschutz-Grundverordnung. DuD: 650-654
- Thoma F. (2013) Risiko im Datenschutz - Stellenwert eines systematischen Risikomanagements in BDSG und DS-GVO-E. ZD: 578-581
- Weichert T. (2013) Wider das Verbot mit Erlaubnisvorbehalt im Datenschutz? DuD: 246-249
- Wieczorek M. (2013) Der räumliche Anwendungsbereich der EU-Datenschutz-Grundverordnung - Ein Vergleich von § 1 Abs. 5 BDSG mit Art. 3 DS-GVO-E. DuD: 644-649

2012

- Bock K, Meissner S. (2012) Datenschutz-Schutzziele im Recht - Zum normativen Gehalt der Datenschutz-Schutzziele. DuD: 425-431
- Caspar J. (2012) Das aufsichtsbehördliche Verfahren nach der EU-Datenschutz-Grundverordnung - Defizite und Alternativregelungen. ZD: 555-558
- Forst G. (2012) Beschäftigtendatenschutz im Kommissionsvorschlag einer EU-Datenschutzverordnung. NZA: 364-367
- Franzen M. (2012) Der Vorschlag für eine EU-Datenschutz-Grundverordnung und der Arbeitnehmerdatenschutz. DuD: 322-326
- Giurgiu A. (2012) Die Modernisierung des europäischen Datenschutzrechts – Was Unternehmen erwartet. CCZ: 226-229
- Gola P. (2012) Beschäftigtendatenschutz und EU-Datenschutz-Grundverordnung. EuZW: 332-336
- Hoeren T. (2012) Der betriebliche Datenschutzbeauftragte - Neuerungen durch die geplante DS-GVO. ZD: 355-358
- Jaspers A. (2012) Die EU-Datenschutz-Grundverordnung - Auswirkungen der EU-Datenschutz-Grundverordnung auf die Datenschutzorganisation des Unternehmens. DuD: 571-575
- Kalabis L, Selzer A. (2012) Das Recht auf Vergessenwerden nach der geplanten EU-Verordnung. DuD: 670-675
- Karg M. (2012) Die Rechtsfigur des personenbezogenen Datums - Ein Anachronismus des Datenschutzes? ZD: 255-260
- Kaufmann NC. (2012) Meldepflichten und Datenschutz-Folgenabschätzung - Kodifizierung neuer Pflichten in der EU-Datenschutz-Grundverordnung. ZD: 358-362
- Kipker DK, Voskamp F. (2012) Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung. DuD: 737-742
- Kugelmann D. (2012) Datenschutz bei Polizei und Justiz - Der Richtlinienvorschlag der Kommission. DuD: 581-583
- Lewinski K. (2012) Europäisierung des Datenschutzrechts - Umsetzungsspielraum des deutschen Gesetzgebers und Entscheidungskomptenz des BVerfG. DuD: 564-570

- Nebel M, Richter P. (2012) Datenschutz bei Internetdiensten nach der DS-GVO - Vergleich der deutschen Rechtslage. ZD: 407-413
- Reding V. (2012) Sieben Grundbausteine der europäischen Datenschutzreform. ZD: 195-198
- Richter P. (2012) Datenschutz durch Technik und die Grundverordnung der EU-Kommission. DuD: 576-580
- Rogall-Grothe C. (2012) Ein neues Datenschutzrecht für Europa. ZRP: 193-196
- Ronellenitsch M. (2012) Fortentwicklung des Datenschutzes - Die Pläne der Europäischen Kommission. DuD: 561-563
- Schild HH, Tinnefeld MT. (2012) Datenschutz in der Union – Gelungene oder missglückte Gesetzentwürfe? DuD: 312-317
- Taupitz J. (2012) Der Entwurf einer europäischen Datenschutz-Grundverordnung – Gefahren für die medizinische Forschung. MedR 30: 423–428
- Wagner E. (2012) Der Entwurf einer Datenschutz-Grundverordnung der Europäischen Kommission. DuD: 676-678
- Wass C, Kurz T. (2012) Digitale Hilfsmittel für mehr Transparenz bei der Verarbeitung personenbezogener Daten. DuD: 748-752

2011

- Hornung G. (2011) Datenschutz durch Technik in Europa - Die Reform der Richtlinie als Chance für ein modernes Datenschutzrecht. ZD: 51-57

16. Abkürzungsverzeichnis

ABl EG	Amtsblatt der Europäischen Gemeinschaften (bis Februar 2003)
ABl EU	Amtsblatt der Europäischen Union (seit Februar 2003)
ABl	Amtsblatt
Abs	Absatz
Art	Artikel
Artt	Artikel (Mehrzahl)
BDSG	Bundesdatenschutzgesetz
DSB	Datenschutzbeauftragter
DS-GVO	Datenschutz-Grundverordnung
EG	Europäische Gemeinschaft
ErwGr	Erwägungsgrund
EU	Europäische Union
grds	grundsätzlich
i.V.m.	in Verbindung mit
Lit	Literal
RL	Richtlinie
Rn	Randnote, -nummer, -zahl, -ziffer
WP	Working Paper